Boran ATES

Master Thesis

Guidelines for "the Implementation of Operational Risk Management"

Studienrichtung:

Production Science and Management

Technische Universität Graz

Published at the
Institute of Production Science and Management
Member of Frank Stronach Institute
Graz University of Technology

○. Univ.-Prof. Dipl.-Ing. Dr. techn. Josef W. Wohinz

Graz, in January 2010

STATUTORY DECLARATION

I declare that I have authored this thesis independently, that I have not used other than the declared sources / resources, and that I have explicitly marked all material which has been quoted either literally or by content from the used sources.

Graz, January 2010 Boran Ates

ACKNOWLEDGEMENTS

Many people have contributed to this work in small and large ways. I am very thankful and thus dedicate this work to…

…Prof. Dr. Josef Wohinz, who is the head of Production Science and Management Institute

…DI Dr. techn. Hannes Fuchs as my research mentor, for your patience, constant guidance and great supportive assistance during my thesis

… DI Dr. techn. Hannes Oberschmid as also my research mentor, for your patience, constant guidance and great supportive assistance during my thesis

…Mehmet Emin Atas and his lovely family, He is my cousin who lives in Graz with his family and has supported and motivated me whenever I needed

…Mehmet Ali Saricicek, who is my grandfather. He passed away on September 2008 but he is going to live in my heart forever. I shall always love you grandpa

…Ali Kutlusoy and Bakk.techn. Emil Marinov who always patiently keep supporting and motivating me during my thesis

…and last but not least, Mustafa, Fatma, Ozan and Ayse Ceren Ates, namely my beloved Family that always believe in me. You are the reason for where and who I am right now. I shall always love you all.

Thank you all!

ABSTRACT

Organisations should focus on the efficiency in every aspect of their operations due to the complexity of nowadays business environment in which the competition is becoming tougher day by day, increased customer demands and market globalisation play a crucial role. In addition to that, organisations which also focus on efficiency of their operations by specifically investing innovation and high-technology lead to market and take the competitive advantage. There are lots of investigations, master thesis and dissertations in operational management that are aimed to improve operational performance, reduce process variability, increase flexibility or implement controls in operations. Nevertheless, organisations still do not take operational risk management or other words to say, managing risks in operational aspect as much serious as they take the other management disciplines.

Moreover, this thesis aims to investigate and describe the Operational Risk Management by defining the State of the Art of Operational Risk Management and broadening the horizon of all kind of risks which are supposed to be related operational, strategic, and financial as well as compliance risks that an organisation faces. Finally, the major result of this thesis is to develop an Operational Risk Management Implementation Process which will guide the organisations to manage all kind of risks they face more effectively, including operational risks. The Operational Risk Management Implementation Process has been supported and put in practice by a Case Study that has been introduced at the end of the thesis.

In order to support the Operational Risk Management Implementation Process, a case study has been introduced at the end of the thesis. Last but not least, this thesis will give a clear opinion to readers regarding Operational Risk Management (ORM) systems and its implementation. It can be also considered as a basis for further researches concerning ORM systems due to it provides comprehensive literature about the approaches of traditional Risk Management as well as ORM. It also gives brief views about Change, Safety, Crisis and Emergency Management disciplines.

TABLE OF CONTENTS

1. INTRODUCTION

The initial situation, objectives, main steps and time schedule of the thesis will be introduced in this chapter.

The brief overview concerning thesis will be explained by mentioning how the topic of thesis has been created as a Master Thesis, what institutions from Graz University of Technology are in charge of the thesis. Furthermore, the objectives, major steps that have been taken during the documentation and investigation processes will be told. Finally, it will be underscored what kind of resources and research materials have been utilised, and when it has been scheduled, begun to be proceed and finalised.

1.1 Initial Situation

The idea of this research has been created and planned as a Master Thesis by the cooperation of the Institute of Production Science and Management (PSM) and Institute of Industrial Management and Innovation Research (IBL) which are the Institutions of Mechanical Engineering and Economics Faculty at Graz University of Technology. The head of both Institutes is o. Univ. Prof. Dipl. - Ing. Dr.techn. Josef W. Wohinz. The supervisors of the thesis from related institutes are DI Dr.techn. Hannes Fuchs and DI Dr.techn. Hannes Oberschmid.

Risk Management and Operational Risk Management which are the major topics of this thesis and also aimed to be taught as a lecture in the near future. Therefore, Risk Management, specifically Operational Risk Management Concept which is a new research branch of Risk Management has been divided into several Master Thesis projects to be given by Institutes of PSM and IBL. Finally, the main topic of the thesis has been determined as Guidelines for the Implementation of Operational Risk Management. The content and the notes of this Master Thesis will be utilized and used as the lecture notes of Operational Risk Management which is planned to be taught at related Institutes, as it was mentioned before.

1.2 Objectives of Thesis

The major objective of this study is to enlighten, and describe the Operational Risk Management by looking deeper through the State of the Art of Operational Risk Management and broadening the horizon of all kind of risks which are supposed to

be related operational, strategic, and financial as well as compliance risks that an organisation faces.

Another objective of the thesis is to give detailed literature and knowledge from both traditional Risk Management and one of its specialised approach so-called Operational Risk Management. These objectives will be explained step by step later on within the related chapters by describing literature, explaining the content of the related subject, mentioning and giving some examples about them as conclusion of each chapter.

Risk Management became one of the most important management disciplines which the organisations must have and pay more attention on it more than ever. Hence, they also have to perform and execute it efficiently and effectively as a whole, if they have an existing Risk Management Concept. If they do not have one, they have to establish a Risk Management Process which allows them to manage all kind of risks both cost-effectively and with minimum effort that they put to reduce or minimize the risks on an tolerable or acceptable level.

Moreover, Risk Management is a kind of complementary management discipline of Total Management Concept like Quality or Project Management, etc. Risk Management allows the organisations to take the competitive advantage on the way of reaching pre-determined organisational goals and objectives, if it is taken and managed as serious and effective as possible like the other management disciplines.

Operational Risk Management is a specialised area of traditional Risk Management which deals with not only the financial risks of the company but also all kind of operative related risks that can occur for example within the production management department or logistics department. It can also affect the other departments, even the finance department, after it occurs. The Operational Risk Management has also become an important part of Risk Management and recently started to play crucial role for organisations. In the near future it will be more and more important than ever for the organisations, because of getting tougher and hardener conditions of nowadays business environment.

The essence of objectives, detailed literature, processes, steps, methodologies and the state of the art of Risk Management as well as Operational Risk Management will be given and explained broadly in the further chapters by the aid of tables, diagrams, figures and case studies in order to be fully understood by readers and industrial practitioners. Once the philosophy and the basic idea of Risk, Risk Management and

Operational Risk Management are correctly understood, it is easy to analyse, monitor, control, mitigate, and manage all risks including operational risks that an organisation encounters along its operations.

1.3 Main Steps and Time Schedule of Thesis

The investigations which are planned as a Master Thesis to be given by the Institutions of Graz University of Technology normally take five to six months to be finalized. The Supervisors of this thesis whom we have talked before about have scheduled this project from the beginning of July until at the end of November. The thesis has been started by a kick-off meeting that has been organised by the supervisors at the first week of July.

In addition to that, there were four check-point meetings that also have been organised by supervisors in order to inform me about the structure, format, procedures, time schedule, and all necessary details of Master Thesis. Besides, my work has been regularly checked, controlled by supervisors in these check-point meetings. The supervisors gave some feedbacks about my work to make me better doing my work. After getting feedbacks and comments about my work, I made necessary corrections right after those check point meetings.

During the time period that I worked on the thesis, I collected required knowledge and literature about my thesis's topic in order to have an idea regarding from where and how I should begin. I therefore borrowed some related books from the library of the Institute of PSM. I also received some reports and articles about Risk and Operational Risk Management from my supervisors. On the one hand, I read all these documents and resources to obtain a certain level of knowledge about Risk and Operational Risk Management. On the other hand, I utilized internet as an effective resource and also read a lot of documents, articles and e-books from various experts and specialists via internet. Furthermore, I utilized some figures, tables, diagrams as well as some definitions as quotations from several books and via internet portals in order to support and make the content of thesis more scientific by the aid of using academicals and expertises point of view.

After working so hard for nearly 6 months, the thesis has been finally completed by the end of December 2009 after all necessary corrections have been made. It has been confirmed on 26th of January 2010 and published on first week of February 2010.

2. RISK MANAGEMENT

The introduction to risk management, definitions of risk and risk management, a brief overview regarding risk management concept according to ISO 31000: 2009, risk management process will be explained comprehensively in this chapter later on.

Moreover, the importance of managing risks will be mentioned for better understanding of why organisations have to pay more attention on the root causes of risks and risk management. At the end of the chapter the brief definitions as well as comparison of risk management, crises management, and safety management will be mentioned in order to let the readers know about the major differences among them and what exactly these management disciplines deal with. Some figures, diagrams, and tables will be utilized and drawn during the chapter for proper definitions and explanations of themes.

2.1 Introduction to Risk Management

Although this thesis aims to emphasise the Guidelines of the Implementation of Operational Risk Management, before we will go further deeply into the aimed topic, the fundamentals of Risk Management Concept has to be clearly identified and understood.

That is why, it is important to know risk and risk management concept from the management, operational as well as the industrial point of views. The Risk management concept has been clearly and comprehensively described as follows within The 2009 Ernst & Young Business Risk Report – The top ten risks in global business; *"In leading organisations, risk management is viewed not as a process, but rather as a "management competency" - a discipline that adds rigor and enables the enhanced management of uncertainty and volatility, effectively minimizes threats and capitalizes on opportunities. Companies at the height of performance in their respective industries have embedded this competency into their business practices to effectively manage risk across the continuum – moving beyond a traditional focus on controls and compliance, to create a competitive advantage."* [1]

[1] Ernst & Young (2009), p. 3

As it was already mentioned in the beginning, this part of thesis is a composed of traditional risk management concept to give a brief overview to the reader and practitioners concerning what risk and risk management are and what they deal with. Detailed and specified knowledge and literatures about the aimed topic of thesis which is known as The Implementation of Operational Risk Management will be given in the following chapters.

2.2 The Definition of Risk

"The word risk has its roots in the old French word risqué, which means "danger, in which there is an element of chance" (Littré, 1863). The word hazard, another term integral to discussions of risk management, comes from a game of chance invented at a castle named Hasart, in Palestine, while it was under siege (Oxford English Dictionary, 1989)" [2]

In order to understand the basics of Risk Management, specifically the Operational Risk Management which an enterprise faces in its day-to-day business, the risk has to be defined and understood correctly by all shop-floor workers, the staff as well as senior managers and board of directors. In other words to say everybody in the organisation from downwards through the top of the organisation has to be fully aware of all retrospective, existing and prospective risks.

Therefore, it would be useful to look at the changing definition of risk in the course of time. Risk is defined as follows according to the International Organization for Standardization's ISO/IEC Guide 73 which has been published in 2002:[3] *"Risk can be defined as the combination of the probability of an event and its consequences".*

According to the Australian & New Zealand Standard on Risk (AS/NZS 4360:2004) which has been recognised internationally as *"better practice"*[4], the risk has been described as follows:[5] *"Chance of something happening that will have an impact on objectives".*

[2] James L. Vesper (2006), Chapter 1, p.1
[3] Patrick Ow (2009), p.6
[4] Victorian Managed Insurance Authority (VMIA) (2009), (Consulted on 05.08.2009)
[5] Patrick Ow (2009), p.6

Lastly, the risk has been re-defined by International Organisation for Standards in the latest version of Risk Management Standard so-called ISO 31000:2009 which will be published on September 2009:[6] *"Effect of uncertainty on objectives".*

In addition, the detailed information about ISO 31000:2009 will be given in the following chapters. As it is mentioned above, in order to make the definitions clear, we have to look at deeper for better understanding of the operative side of the risks in an organisation; we have to clarify the risk definition both from the engineering and more general point of views.

"In engineering, the definition risk is often simply:

Risk = (probability of an accident) x (losses per accident)

Or in more general terms:

Risk = (probability of an event occurring) x (impact of event occurring)"[7]

As a result of collecting all above-mentioned definitions in accordance with industrial, engineering and management point of views, the risk can be generally described as an event which has a probability to occur that can carry either a negative impact so-called "threat" or a positive impact so-called "opportunity" to an enterprise.

The types of risks and the top ten business risks have been classified and named as follows by Ernst & Young in their business risk report which is so-called The 2009 Ernst & Young Business Risk Report – The top ten risks in global business. The Figure 1 illustrates the risk classification as well as the top ten business risks across the 11 core industry sectors like Asset Management, Automotive, Banking, Consumer Products, Insurance, Oil and Gas, Real Estate, Telecoms and etc. that Ernst & Young covered.

[6] Patrick Ow (2009), p.6
[7] Wikipedia, (Consulted on 25.07.2009)

Figure 1 – the top 10 Business Risks[8]

Finally, it has to be pronounced once again that this study will focus on more the operational risks and the implementation of operational risk management which are more related to industrial activities than the other kinds of risks, for example financial or credit risks. Financial risks are more related to banking and insurance sectors which we are not going into further in this research. These sectors are not really connected with the operational and industrial practices, such as supply chain, production, project management and etc. that we are exactly aiming to guide the readers and practitioners in this research about.

2.3 The Importance of Managing Risks

In order to fully understand the importance of managing risks, the benefits of managing risks have to be introduced and embedded. Thereby, we will be able to understand what benefits will be brought into an organization and what advantages

[8] Ernst & Young (2009), p. 4

will be taken by the organization, if all possible risks that an organization faces, are correctly and successfully managed.

Before we start to explain why it is important to manage risks, an important observation of one the worldwide-known financial newspapers has to be promoted here concerning the importance of Managing Risks as well as Risk Management. *"Managing risk is one of the things that bosses are paid for," yet "most companies still don't have any idea what is required of risk management," stated The Economist (2004).*[9]

Therewith, it will be vital and useful to mention the advantages which the organisations take when they manage their risks effectively or they implement an effective risk management concept along their operations. These advantages or the help of Effective Risk Management are determined by British Standards Institution (BSI) in their Risk Management Standard which is considered a key standard for risk management.

BS 31100:2008 gives organisations a view and understanding on how they can develop, implement and maintain an effective risk management to their business. It also allows the organisations to increase their businesses' effectiveness. It also ensures to understand the importance of managing risks, if the organisations implement this standard to their businesses appropriately, and effectively.

"Effective risk management help you achieve your objectives by:[10]

a) *Reducing the likelihood of events that would have a negative impact on your business*

b) *Increasing the likelihood of events that would have a positive impact on your business*

c) *Identifying opportunities where taking risks might benefit your business*

d) *Improving accountability, decision making, transparency and visibility*

e) *Identifying, understanding and managing multiple and cross-organisation risks*

f) *Executing change more effectively and efficiently and improving project management*

[9] James L. Vesper (2006), Chapter 1, p. 8
[10] British Standards Institution (2008), (Consulted on 27.08.2009)

g) *Providing better understanding of, and compliance with, relevant governance, legal and regulatory requirements, and corporate social responsibility and ethical requirements*

h) *Protecting your revenue and enhancing value for money*

i) *Protecting your reputation and stakeholder confidence*

j) *Proactively managing your organisation's operations*

k) *Controlling expenditure and delivering a cost-optimal control environment*

l) *Retaining and developing customers by being more flexible and responsive to their needs*

m) *Making the organisation more flexible and responsive to market fluctuations so that it is better able to satisfy customers' ever-changing needs in a continually evolving business environment."*

The concept of risk has been explained so far in order to have an idea about what risk is, what it stands for, what can be considered as a risk, what are the profits of well-managed risks on behalf of organisations. The concept of Risk Management will be detailed and explained in the following chapter. It is always an advantage to know for the managers or especially risk managers/risk officers what kind of current or prospective problems in terms of risks they will face or what kind of problems can be considered as risks with their possible positive or negative impacts on the pre-determined objectives of the organisation.

2.4 Risk Management Definitions

The risk management and its applications are more essential than ever for organisations. It progressively becomes one of the most important and must be had management disciplines in an organization, especially nowadays business environment in which the perfection of business mechanism within the organization is required. That means all departments of an organisation should collaborate efficiently and effectively with each other and all operations are done without facing any problems or risks that block the perfection of business mechanism of the organization and bring some troubles to organisations in terms of quantitative and qualitative results like losing money, market share, even the reputation of company and etc.

It is very important to do everything correctly and in an appropriate manner in order to take the competitive advantage to lead the sector for today's business. Therefore, the companies have started to pay more attention on Risk Management, comprehensively not only the financial understanding of Risk Management, but also the operational understanding of Risk Management related supply chain risk management, enterprise risk management, project risk management and etc. In other word to define; the organisational risk management which an organisation faces all kinds of risks, as mentioned above, financial, operational, engineering, business, even environmental, and etc.

Risk Management has become more important for organisations in the middle of 1990s after some financial losses in terms of tons of dollars and some banking collapses. That was the time risk management was dominantly related to finance, banking and insurance sectors. But just 10 years later, the organisations have realised that the concept of risk management can include the other parts of a business and risk can occur any part of a business with irretrievable monetary losses, bankruptcies due to these monetary loses, and even losses of human lives.

The companies have noticed this issue after some dramatically happened accidents, failures or disasters like the largest supplier of mobile telecom systems of the world; Ericsson has had this kind of an accident on 18 March 2000. The accident has happened as follows:[11] That was a major accident from an Ericsson perspective which occurred as a fire in a very small production cell (small as a conference room for ten people) at a sub-supplier's plant in Albuquerque, New Mexico/USA. The fire continued only ten minutes, and it has happened due to an effect of a lighting bolt hitting an electric line in New Mexico, and caused power fluctuations along the state. The problem was that the fans stopped, because there were no auxiliary diesel motors which provide the fans with power, when the power was out. According to Wall Street Journal, the fire might be ignored from a plant point of view, because it took just ten minutes and the fire workers was sent home, after they arrived to the plant because the fire was extinguished. But the impact of the fire could not be ignored by Ericsson, because it was enormous in terms of monetary loss. The loss was readily realised, when the annual report from Ericsson was issued in the spring of 2001; the major loss was about $400 million which mainly caused by the gaps in the supply of radio-frequency chips from this supplier. The root cause of the fire which happened in one of the plant's clean rooms, where exactly no dust is tolerated.

[11] Cf: Ericsson (2004), p.5

The starting up of production and its running took almost three weeks due to the fire, and especially the smoke and the sprinkler water. The efficiency after six months was only 50 percent and getting new equipments and their installation would take years. Ericsson was not capable to sell and deliver one of its key consumer products during its booming market window, because this sub-supplier so-called this plant was the only supplier for this chip. As a consequence, Ericsson could not produce any mobile phones for many months, and the fire finally had a great impact on Ericsson's decision to withdraw from the mobile phone terminal business.

Afterwards, Ericsson's business interruption costs were calculated as nearly $200 million, which was compensated by insurance companies and was one of the biggest insurance payments after 9/11 disaster. After the accident, Ericsson realised the importance of not only understanding and managing risks internally, but also trying to better analyse, assess and execute risks throughout the supply chain and to take immediate actions when an accident occurs. According to The Wall Street Journal and the general thought regarding the accident was that Ericsson did not act quickly sufficiently after the accident, top management's awareness about the incident took so long. In addition to that, Ericsson had no alternative suppliers, and they were not well prepared for that kind of accidents. After that accident, some lessons have been learned by Ericsson, and some actions have been taken afterwards: During the last couple of years, a formal Supply Chain Risk Management (SCRM) Organisation has been put in practice, and may SCRM processes, tools, and methods have been developed and implemented by Ericsson. Today's philosophy at Ericsson is that everybody is a risk manager within the organisation.

There can be found thousands of Risk Management definitions via internet or by published books. These definitions can be varying from author to author or according to what type of risks will be related with your business. Therefore, the very fresh issued definitions of risk management will be described here from the very general point of risk management view.

Risk management is defined as follows by Douglas Hubbard in his recently issued book of "The Failure of Risk Management: Why It's Broken and How to Fix It":[12] "*Risk management is the identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events".*

[12] Douglas W. Hubbard (2009), p.46

The remarkable risk management definition of Peter L. Bernstein who is recognised as *"the father of risk"* [13] and *"one of the true Renaissance men of the finance world"* [14] by most finance professors from important universities around the world as well as Chief Finance Officers (CFOs) and economists of the largest enterprises, make the concept of risk management an important key management discipline for the organisations.

Bruce McDougall who is the president of Brucer Media Inc. Canada has mentioned his meaningful opinions about Peter L. Bernstein after his death as follows:[15] *"Thanks for this. Peter Bernstein has done for risk what Charles Darwin did for evolution. I admire him without reservation".*

Peter L. Bernstein's book which is named "Against the Gods" which has revolutionary broaden the perspective of risk and risk management and has been recognised as a milestone of risk management by authorities. He described risk management in his book as follows:[16] *"The essence of risk management lies in maximizing the areas where we have some control over the outcome while minimizing the areas where we have absolutely no control over the outcome and the linkage between effect and cause is hidden from us".*

Before the conclusion of this chapter, it would be vital and helpful here to mention about some steps through better risk management which should be taken by organisations in order to create an appropriate and effective risk management concept.

These ten steps to better risk management are noted below:[17]

1. *Risk management must be given greater authority.*
2. *Senior executives must lead risk management from the top.*
3. *Institutions need to review the level of risk expertise in their organisation, particularly at the highest levels.*
4. *Institutions should pay more attention to the data that populates risk models, and must combine this output with human judgment.*

[13] R.I.P. Peter L. Bernstein – Father of Risk (2009), (Consulted on 02.08.2009)
[14] Mustafa Gültekin (2009), (Consulted on 02.08.2009)
[15] Bruce McDougall (2009), (Consulted on 02.08.2009)
[16] Peter L. Bernstein (1998), p.197
[17] Victorian Managed Insurance Authority (VMIA) (2009), p.8

5. *Stress testing and scenario planning can arm executives with an appropriate response to events.*
6. *Incentive systems must be constructed so that they reward long-term stability, not short-term profit.*
7. *Risk factors should be consolidated across all the institutions operations.*
8. *Institutions should ensure that they do not rely too heavily on data from external providers.*
9. *A careful balance must be struck between the centralisation and decentralisation of risk.*
10. *Risk management systems should be adaptive rather than static.*

As a conclusion of Risk Management and putting all definitions together which are mentioned by now. Risk Management should be a part of Total Management System which consists of several steps like identifying, analysing, evaluating and treating risks according to a certain risk management process with the cooperation and effective communication of other management disciplines during the operations in order to create profit, value and have competitive advantage by minimizing threats and maximizing opportunities that an organisation faces. Once the concept of risk management has been identified, the very crucial point of risk management will appear. This will be the answer of the question of how the risk management will be operated, implemented and tailored to a business or an organisation in terms of operational risk management. But before we do that, a brief literature and knowledge regarding ISO 31000:2009 will be given next.

2.5 Risk Management according to ISO 31000:2009

As it has been mentioned previously, there can be done hundreds of risk management definitions, but it is important to know the application area of risk management from the revised document/standard of International Organisation for Standardisation so-called ISO 31000:2009 which is specifically prepared and considered as the first international standard on risk management. ISO 31000:2009 defines the application area of risk management as follows:[18] *"Risk management can be applied to an entire organisation, at its many areas and levels, at any time, as well as to specific functions, projects and activities."*

[18] Victorian Managed Insurance Authority (VMIA) (2009), (Consulted on 05.08.2009)

In addition to that, it is further necessary to say what the new standard deals with, and why it has been needed to be revised and developed. All these questions are briefly answered as follows:[19] *"ISO 31000:2009 is the first international standard on risk management that clearly and explicitly sets out the principles and framework for managing risk. The standard intends to harmonise risk management processes in existing and future standards. It provides a common approach to dealing with specific risk and/or sectors, and does not replace pre-existing relevant standards.*

In conjunction with developing ISO 31000, the ISO Risk Management Working Group is updating "ISO/IEC Guide 73, Risk Management – Vocabulary" that will provide a glossary of risk management terms. The guide aims to develop a consistent language relating to the management of risk".

ISO 31000:2009 is at its final stage to be approved at the moment and it is expected to be issued in September 2009.

2.6 Risk Management Process

The concept of risk and risk management have broadly described by now in order to make their definitions clear and better understanding as well as embedding risk management process which will be detailed in this chapter.

Risk Management Process is eventually a process itself which basically has an input that is transformed by the process and an output as the result that is produced by process, like other regular processes and it is simply shown in Figure 2 below.

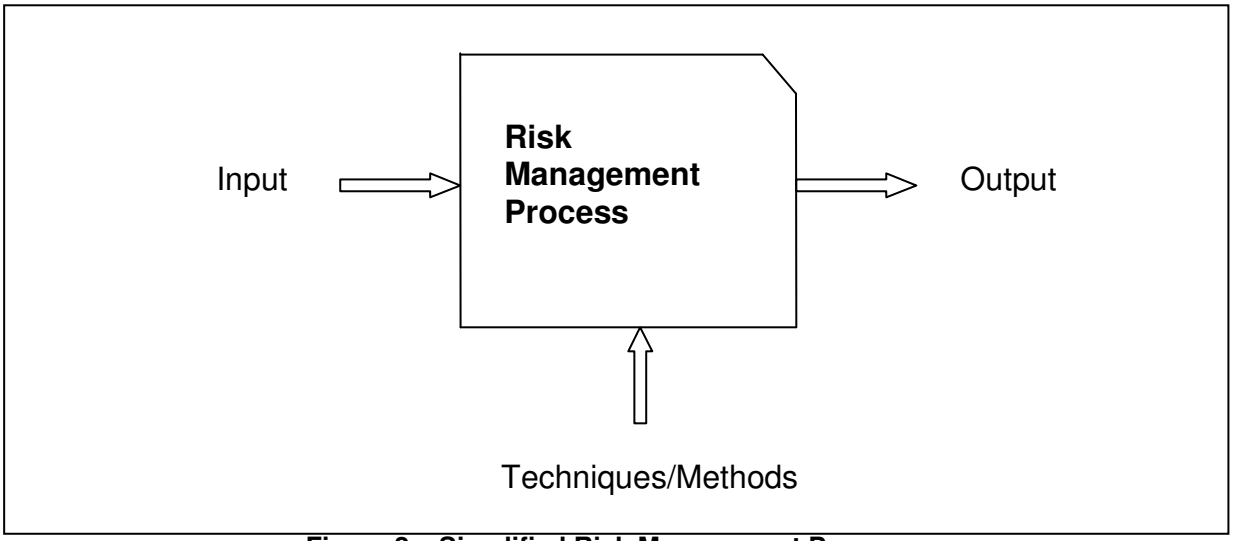


Figure 2 – Simplified Risk Management Process

[19] Patrick Ow (2009), p.5

Moreover, there are some techniques and methods which are applied during the process and may be used to support the completion of the process. These methods will be mentioned and detailed in the following chapters. Risk management process consists of various steps that are connected with each other. When they are sequentially implemented, they enable continual improvement in decision-making.

The risk management process is divided in seven major steps. Each step will be described comprehensively later on in order to make clear the importance of each step and the entire risk management process as well as its contribution to organisation. These steps are named as follows and will be illustrated in Figure 3 below:

- Step 1. Stakeholder Dialogue – Communication/Consultation
- Step 2. Establish the context
- Step 3. Identify the risks
- Step 4. Analyze the risks
- Step 5. Evaluate the risks
- Step 6. Treat the risks
- Step 7. Monitoring and review

Meanwhile, different risk management processes or risk management cycles can be illustrated and shown by using different types of figures. These processes' steps and their illustrations have been made by different authors, finance professors and experts. They all more or less agree with some basic steps of risk management. Once they have been named, the next step will be the right understanding of each step by going deeply into them.

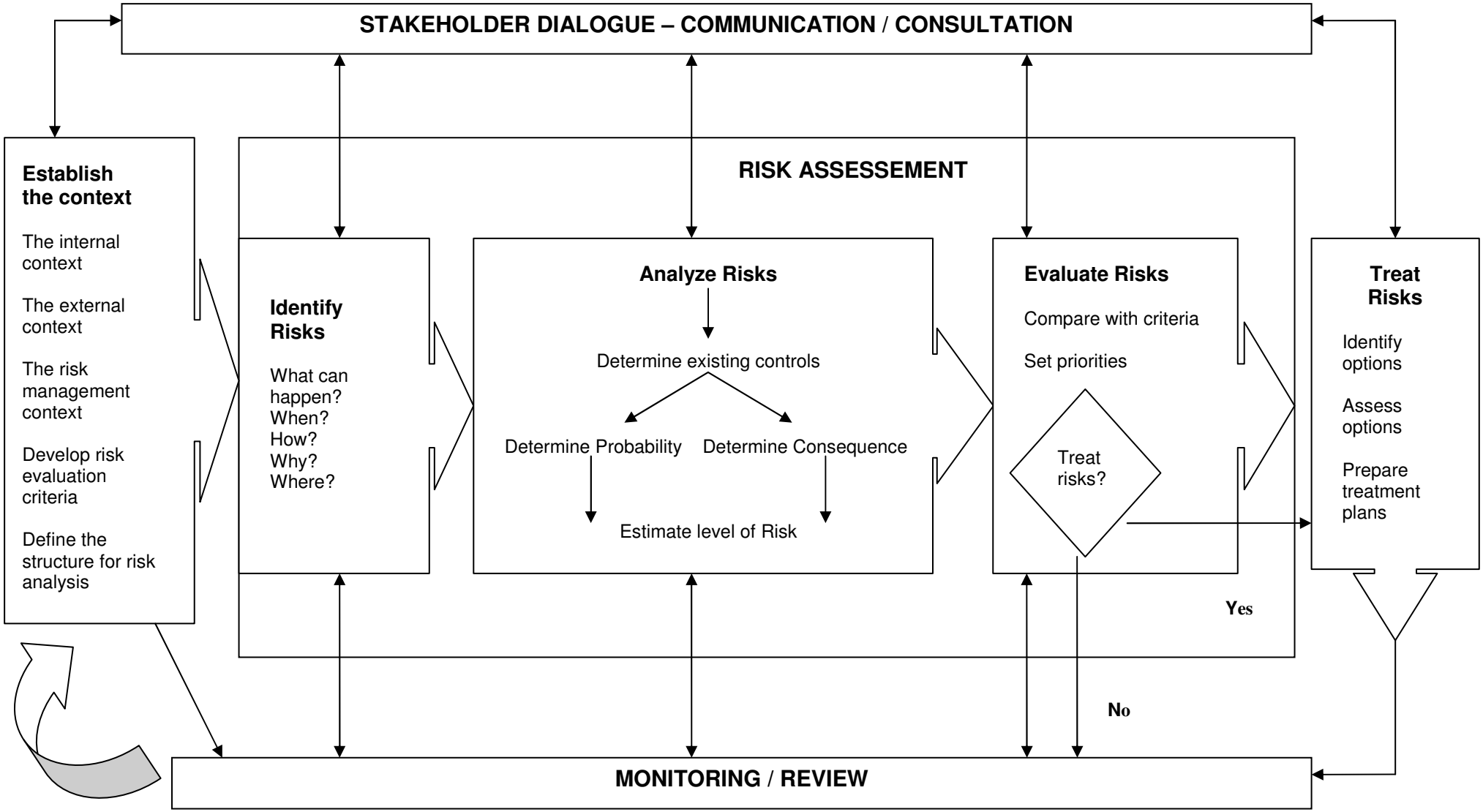


Figure 3 – Risk Management Process[20]

[20] Cf: AS/NZS 4360:2004, p.39 and Australian Agency for International Development (AusGuideline), p.5

2.6.1 Step 1: Stakeholder Dialogue – Communication/Consultation

The first step of risk management process is actually one of the most important steps of the entire process. The organisations have to make sure that the stakeholder dialogue, communication and consultation have to be implemented and successfully executed throughout the organisation in order to ensure that all personnel and stakeholders are properly informed at all stages of the process. Hence, this step should be put in practice at each step during the whole process. That is why; it is a kind of complementary stage of the entire process as it was shown in Figure 3 above.

Effective internal and external communication is crucial and targets to determine the responsible person of risk assessment (including the identification, analysis and evaluation). In order to make sure that the effective communication works correctly, a communication strategy/plan has to be implemented as fast as possible within the process. The communication can be whether personnel wants to communicate with management or the management wants to communicate with the personnel. The opportunities for communication for both sides have to be provided and must remain open to have a transparent communicational system with both external and internal person addressed of the organisation.

"As an initial step, there are two main aspects that should be identified in order to establish the requirements for the remainder of the process. These are communication and consultation aimed at:

- *Eliciting risk information*
- *Managing stakeholder perceptions for management of risk.*

Eliciting Risk Information

It is very rare that only one person will hold all the information needed to identify the risks to a business or even to an activity or project. It is therefore important to identify the range of stakeholders who will assist in making this information complete.

Consultation is a two-way process that typically involves taking to a range of relevant groups and exchanging information and views. It can provide access to information that would not be available otherwise." [21]

Managing stakeholder perceptions for management of risk

The stakeholders related risk management processes are the individuals who may affect or are affected by any of decisions that an organization takes during risk management process. The exact number of stakeholders of a business depends on the size and type of the business. Figure 4 shows the Stakeholders in a small-sized business.

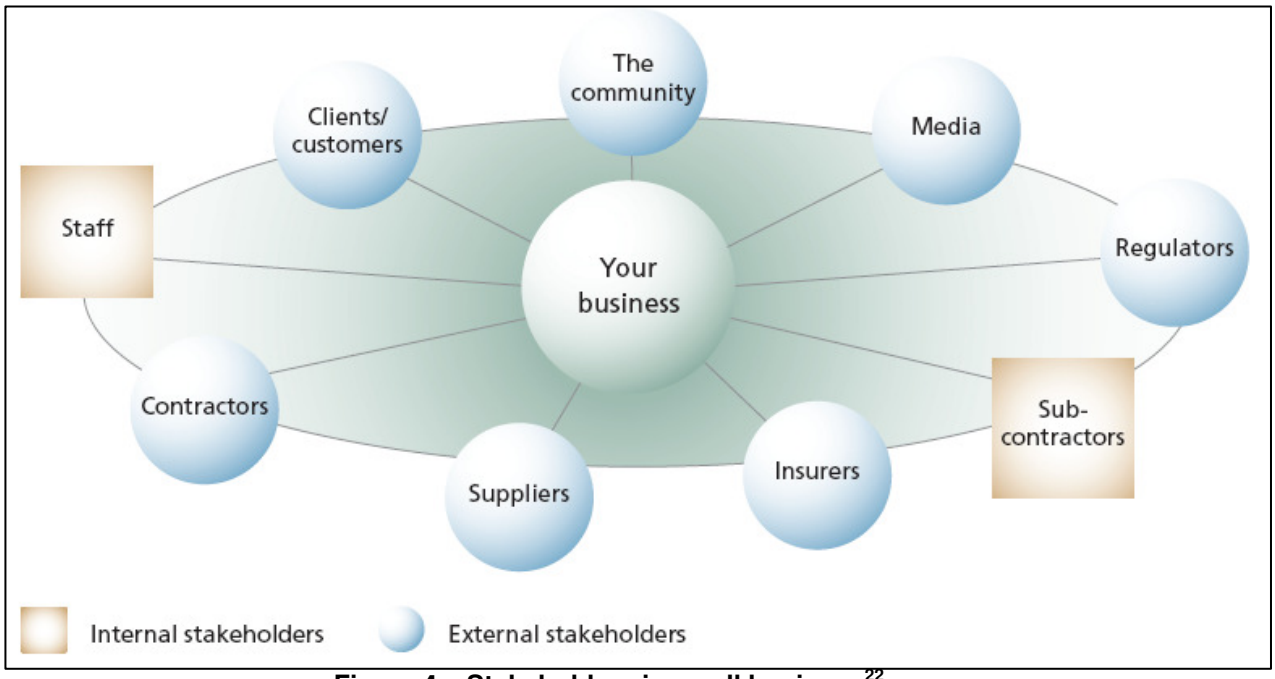


Figure 4 – Stakeholders in small business[22]

"Stakeholder management can often be one of the most difficult tasks in business management. It is important that stakeholders are clearly identified and communicated with throughout the risk management process. They can have a significant role in the decision-making process, so their perceptions of risks, as well as their perceptions of benefits, should be identified, understood, recorded and addressed". [23]

[21] Global Risk Alliance Pty. Ltd. jointly with New South Wales (NSW) Department of State and Regional Development (2005), p.22
[22] Global Risk Alliance Pty. Ltd. jointly with NSW Department of State and Regional Development (2005), p.23
[23] Global Risk Alliance Pty. Ltd. jointly with NSW Department of State and Regional Development (2005), p.23

2.6.2 Step 2: Establish the Context

Establishing the context is divided into 5 sub-steps as it has been shown in Figure 3 before. These sub-steps have to be defined properly, and fully understood during the entire step in order to make all risks clear that an organisation faces. That will ensure afterwards the risk management team - including stakeholders, risk staff and risk managers - to have the exact and correct decision making-processes as well as strategic thinking capabilities. Because as stated in the AS/NZS 4360:2004 (Australian/New Zealand Risk Management Standard):[24] *"Establish the context; establish the strategic, organisational and risk management context in which the rest of the process will take place".*

In order to establish above-mentioned context, the divided 5 sub-steps are named as follows:

1. The internal context
2. The external context
3. The risk management context
4. Develop risk evaluation criteria
5. Define the structure for risk analysis

1. The internal context

The establishment of the internal context is about risk issues which an organization has to clarify internally and make sure whether they are able or ready to deal with risk management process as well as the establishment of the context step. In order to ensure that the internal context has been well set up during the whole context establishment step, organisations have to audit and examine themselves.

The organisations have to ask some internal questions to them. They have to find out some points concerning the internal context by answering some important questions like whether they have a corporate culture to react against risks as a whole or not. If not, how they have handled the risks they have faced retrospectively, they have an existing risk management team or not, what teams they have already in terms of other management disciplines except risk management. Is there an existing change management process within the organisation which has been successfully implemented and works appropriately when it is needed or not. If not, how it should

[24] Australian Capital Territory Procurement Circular (2009), p.2

be implemented in order to minimize the resistance against any changes within the organisation. Besides, how hard to change something or how is the resistance reactions against changes from staff, senior managers, even the Board of Directors.

In addition, the organisations have to make sure that what existing abilities they have already or what capabilities they do not have to treat risks when they have some risks which negatively affect the organisational objectives. These abilities can be evaluated in terms of people, technologies, machines, processes, systems, and etc.

2. The external context

The external context refers to the external environment in which an organisation operates. The external environments can be considered as legislative, regulatory political, cultural, socio-economic and etc. In this step organisations have to determine what external factors of their external environment improve or hinder to reach the pre-determined strategic objectives of the organisation.

The external context should include all participations from the external environment of an organisation as well as the internal stakeholders. Therefore, the internal and external stakeholders and their involvement within the risk management process have to be identified. The relationship and communication between those stakeholders and the organisation have to be managed appropriately.

Lastly, once again organisations have to examine themselves at this stage in terms of external factor which will probably affect the organisation. As it was mentioned before, these factors can be regulatory, legislative, social and etc. These factors have to be seriously taken into account by organisations. The organisations have to comply with some legislations, regulations and standards that they have to obey in order to have the competitive advantage. They also have to find out what additional requirements are needed to be completed or what the market conditions are in which they currently operate, what the market requirements are right now and how they will be in the future. Moreover, organisations should determine who the existing competitors as well as new entrants are and how organisations can compete with them in a short, middle as well as long-term period.

3. The risk management context

The risk management context has been defined by the State of Queensland/Australia as follows; *"Establishing the risk management context defines the activity or issue under scrutiny that and includes the objectives, scope, boundaries and agencies' business units involved"* [25]

It is necessary to clearly identify the parameters for this activity to ensure that all important risks are identified. These clearly identified parameters and boundaries of the activity of risk management process involve:[26]

- *Define risk project scope and parameters;*
- *Define risk management extent in time and location;*
- *Identify any studies needed;*
- *Identify resources needed (Human Resources, Financial Resources and IT Resources);*
- *Risk budget – need to balance costs, benefits and opportunities; and*
- *Specific issues (Special roles and responsibilities, Risk Project/Risk Project Dependences)*

Finally, it is also useful to mention about some tips for establishing the risk management context. These tips have been given as follows:[27]

- *Define the objectives of the activity, task or function*
- *Identify any legislation, regulation, policies or standards and operating procedures that need to be complied with*
- *Decide on depth of analysis required and allocate resources accordingly*
- *Decide what the output of the process will be, e.g. a risk assessment, job safety analysis, or a board presentation. The output will determine the most appropriate structure and type of documentation.*
- *…*

[25] Queensland Government – Property Management Committee (2009), (Consulted on 08.08.2009)
[26] Queensland Government – Property Management Committee (2009), (Consulted on 08.08.2009)
[27] Global Risk Alliance Pty. Ltd. jointly with NSW Department of State and Regional Development (2005), p.25

4. Develop risk evaluation criteria

The risk criterion determines whether the selected change in an organisation is considered an acceptable or an unacceptable change. The change can be identified a potential risk which may affect negatively or positively on the pre-determined organisational objectives. Therefore, the acceptable and unacceptable level of risk has to be identified as well as what is acceptable and what is unacceptable has to be determined at this stage.

If risk decreases due to change, then the change or risk is accepted. On the one hand the change cannot be accepted or can be considered an unacceptable one, if it brings significant qualitative or quantitative impacts on the organisation. On the other hand, some changes may be accepted in a negligible manner due to some other benefits that they overcome, in spite of the risk increases because of change.

Finally, the responsible person for accepting risk has to be determined at this stage as well. Table 1 shows some examples of risk criteria for a project in a small business.

Risk Criterion	***Objective***
Safety	*Safety must be upheld at all times. No injuries or fatalities will be accepted*
Financial impact	*Project cost should remain within allocated budget*
Media exposure	*The project must ensure that the reputation of the business is protected from the negative media exposure*
Timing	*The project must be completed within the contractual timeframe*
Staff management	*The 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 with the business's environmental commitment*

Table 1 - Examples of risk criteria for a project in a small business[28]

[28] Global Risk Alliance Pty. Ltd. jointly with NSW Department of State and Regional Development (2005), p.26

5. Define the structure for risk analysis

This is the last sub-step of the context establishment step. It is also the determination step of the structure for risk analysis which will be implemented later on. The determined structure for risk analysis varies according to the type of the event as well as the context and complexity of it.

The structure for risk analysis allows organisations to take the advantage of identifying significant risks properly, because of the deeply and accurately determination abilities of it.

2.6.3 Step 3: Identify the Risks

It is essential to identify the risks clearly in order to manage them properly. Therefore, one aim of identifying risks' step is to ensure that no significant risk is inspected and try to define as much risks as possible that an organisation faces. Once this process can be achieved, then risks can be easily analysed and evaluated too.

Some risks and hazards are readily to detect. Conversely, there are some risks which cannot be identified, estimated or seen easily. It is compulsory at this stage that organisations make sure that all possible risks are identified. Thus, organisations should ask some questions to themselves in order to clarify all possible risks which may occur. These questions are as follows:

- What could happen?
- When and where could it happen?
- How and why could it happen?
- How can we prevent and minimize risks?
- …

The other aim of risk identification is to develop a comprehensive list of risks that impact on organisational objectives. Effective risk identification needs personal experience, judgment as well as expert knowledge of the subject.

"There are two main ways to identify the risks:[29]

- *Retrospectively*
- *Prospectively*

Identifying retrospective risks

Retrospective risks are those that have previously occurred, such as incidents or accidents. Retrospective risk identification is often the most common way to identify risk, and the easiest one. It is also easier to quantify its impact and to see the damage it has caused.

There are many sources of information about retrospective risk. These include:

- *hazard or incident logs or registers*
- *audit reports*
- *customer complaints*
- *accreditation documents and reports*
- *past staff or client surveys*
- *Newspapers or professional media, such as journals or websites.*
- *…*

Identifying prospective risks

Prospective risks are often harder to identify. These are things that have not happened yet, but might happen sometime in the future.

Identification should include all risks, whether or not they are currently being managed. The rationale here is to record all significant risks and monitor or review the effectiveness of their control.

Methods for identifying prospective risks include:

- *brainstorming with staff or external stakeholders*
- *researching the economic, political, legislative and operating environment*
- *conducting interviews with relevant people and/or organisations*

[29] Global Risk Alliance Pty. Ltd. jointly with NSW Department of State and Regional Development (2005), p.28

- *undertaking surveys of staff or clients to identify anticipated issues or problems*
- *flow charting a process*
- *Reviewing system design or preparing system analysis techniques.*
- *…"*

SWOT Analysis is one of the most effectively used prospective risk identification tools. A sample SWOT analysis for a plumbing business is shown in Figure 5.

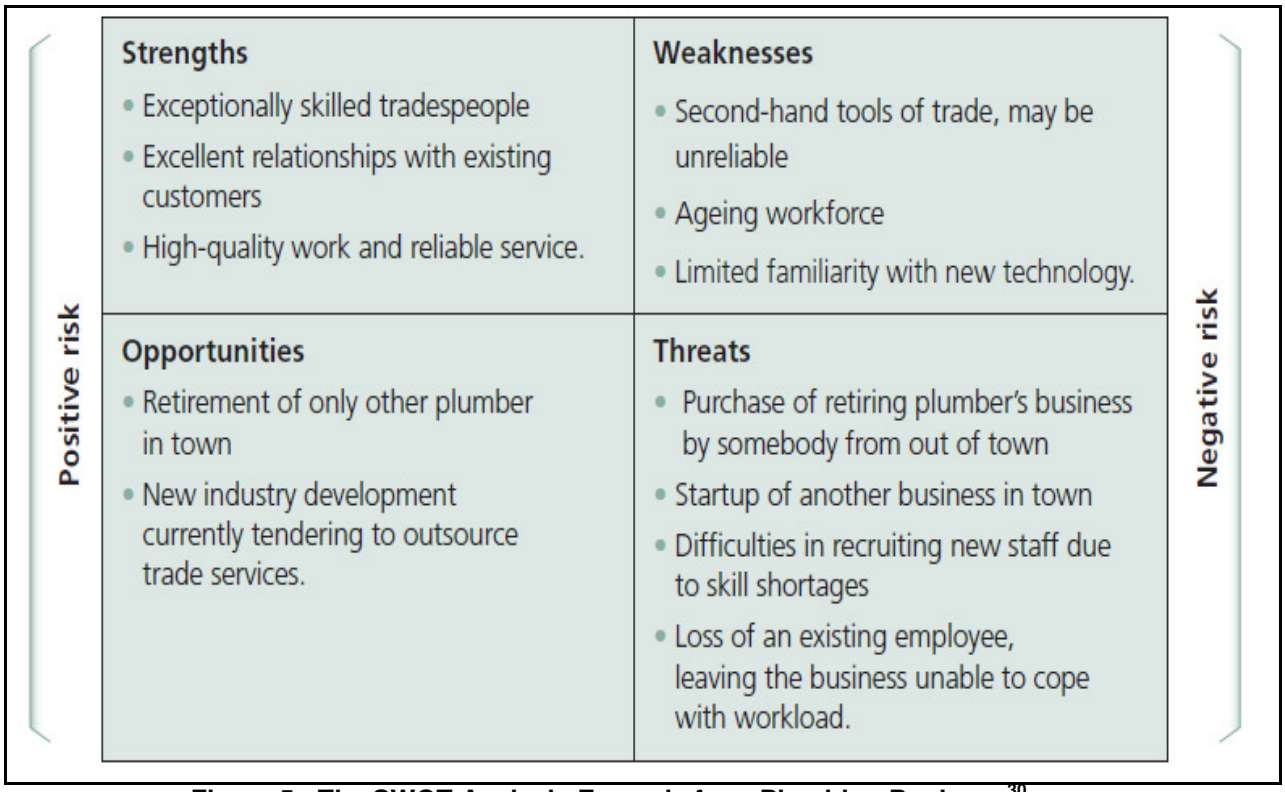


Figure 5 - The SWOT Analysis Example for a Plumbing Business[30]

2.6.4 Step 4: Analyse the Risks

Once the risk has been identified broadly and properly, then risk has to be analysed in order to get ready to be evaluated, prioritised and treated for following steps. The risk analysing step aims to determine what risks have larger and more important impacts or consequences than the others. In order to have an idea regarding fundamentals of this step, the question of what risk analysis is, should be briefly enlightened.

[30] Global Risk Alliance Pty. Ltd. jointly with NSW Department of State and Regional Development (2005), p.29

The Definition of Risk Analysis

Several risk definitions have been made in the very beginning of this study. Meanwhile, the risk analysis equation can be re-defined as follows:[31]

"Risk = Consequence x Likelihood"

As it is shown on the formula above, the result of formula determines the level of risk and risk analysis is a practice of consequence and likelihood. Once the risk analysis has been understood, the question of how the level of risk will be determined is arisen.

"Elements of risk analysis"[32]

The elements of risk analysis are as follows:

1. Identify existing strategies and controls that act to minimise negative risk and enhance opportunities.

2. Determine the consequences of a negative impact or an opportunity (These may be positive or negative).

3. Determine the likelihood of a negative consequence or an opportunity.

4. Estimate the level of risk by combining consequence and likelihood.

5. Consider and identify any uncertainties in the estimates.

1. Identify existing strategies and controls that act to minimise negative risk and enhance opportunities

This is the element of risk analysis which the concept of possible impact of risk is obviously ensured. The existing strategies and controls have to be defined in order to be implemented afterwards. Conversely, there are always some risks which remain, although several preventions are taken and operated against these risks. The

[31] Global Risk Alliance Pty. Ltd. jointly with NSW Department of State and Regional Development (2005), p.30
[32] Global Risk Alliance Pty. Ltd. jointly with NSW Department of State and Regional Development (2005), p.30

magnitude of the remained risks has to be determined as well, after the existing strategies and control measures are identified.

We can give some examples regarding remained risks. For example, fastening seat-belt before driving or buying a car which is fully equipped in terms of crash safety equipments (air bags, ABS, seat-belt and etc.) do not prevent the probability of a possible death after having an accident or a crash. There are still some risk as residual risks which cause a possible death or injuries, even though some precautions have been taken before.

2. Determine the consequences of a negative impact or an opportunity (These may be positive or negative)

"Consequences are the possible outcomes or impacts of an event. They can be positive or negative, and can be expressed in quantitative or qualitative terms and are considered in relation to the achievement of objectives".[33]

By the way, it would be useful to introduce an example here for better understanding of the determination of consequences of a negative impact or an opportunity. Not using a welding mask/glass during the welding operation causes eye strain, amblyopia (defect of vision) or even the lose of eye(s) of welding operator. These possible losses or injuries are considered as the consequences of not using a welding mask/glass during operation. It is therefore important for organisations that they have to ensure that the estimation of potential loss (risk) has to be done precisely.

3. Determine the likelihood of a negative consequence or an opportunity

"Likelihood relates to how likely an event is to occur and its frequency.

An example is the likelihood that a non-maintained piece of machinery will malfunction and result in major injury requiring hospitalisation, or possible death, of an employee.

Likelihood = probability x exposure

[33] Global Risk Alliance Pty. Ltd. jointly with NSW Department of State and Regional Development (2005), p.30

Likelihood relates to the probability of a risk occurring combined with the exposure to the risk." [34]

In order to make the above-mentioned formula clear, an example from industry can be explained. For example, an exporting company which is currently successful and makes profit due to lack of competition within the existing market in which it operates. Its probability of being successful within the existing market is (would be) therefore higher than entering a new market. New market means more effort to be put and more money to be spent for promotions.

On the other hand, there are some new entrants as competitors appeared in the market in which the exporting company currently and successfully operates. Some times later the success of the exporting company has explicitly decreased because of strong and effective competition exposure by new entrants. The new entrants swiftly became serious competitors by appropriately integrating the market changes, taking the advantage of innovation and new technologies and thereby reducing the prices which still make profit and are less than the exporting company offers.

4. Estimate the level of risk by combining consequence and likelihood

As it was previously mentioned, risk has been re-formulated with combining the consequence of a risk and likelihood of a risk occurring. The outcome of the related formula so-called risk analysis equation results the level of risk, as it was introduced before.

The estimation level of risk is usually determined by using Risk Analysis Matrix, Risk Descriptors, mathematically described values and etc. Risk Analysis Matrix will be broadly introduced here in order to have an overview how the level of risk is estimated.

The risk matrices are used to aid decision analysis. It consists of a two dimensional representation. The Qualitative Risk Analysis Matrix is illustrated on Table 2 as follows:

[34] Global Risk Alliance Pty. Ltd. jointly with NSW Department of State and Regional Development (2005), p.31

Qualitative Risk Analysis Matrix - Level of Risk *

Likelihood	Consequences				
	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
A (almost certain)	M	H	H	E	E
B (likely)	M	M	H	H	E
C (possible)	L	M	M	H	E
D (unlikely)	L	M	M	M	H
E (rare)	L	L	M	M	M

Table 2 – Qualitative Risk Analysis Matrix – Level of Risk[35]

* ***Level of risk:***

(E) ***Extreme risk*** *– Immediate action required. Senior Executive Management attention needed with action plans or response procedures and management responsibility specified. All possible treatments to be put in place to reduce risk*

(H) ***High risk*** *– Senior Management action required, risk treatments applied. Responsibility must be specified. Subject to regular monitoring*

(M) ***Moderate risk*** *– Must be brought to attention of manager. Manage by specific monitoring, or response procedures, with Management responsibility specified.*

(L) ***Low risk*** *– Manage by routine procedures, unlikely to need specific application of resources.*

[35] Australian Capital Territory Procurement Circular (2009), p.5

Qualitative measures of consequence (with examples)[36]

(1) ***Insignificant*** *- No injuries, low financial implications.*

(2) ***Minor*** *- Possible injury not more than first aid treatment, medium financial loss.*

(3) ***Moderate*** *- Possible injuries would require medical treatment, high financial loss.*

(4) ***Major*** *- Extensive injuries possible, major financial loss.*

(5) ***Catastrophic*** *- Death is clearly possible, huge financial implications.*

The likelihood of an event occurring again or of causing harm[37]

Descriptor	***Likelihood of recurrence – Effectiveness of existing control measures***
Almost certain (A)	*This event will occur again. It is a persistent issue. e.g. Daily, Weekly or Monthly. No control measures thus constant exposure.*
Likely (B)	*This event will occur again at some time e.g. Every 2/3 months. Poor training, lack of supervision or ineffective control in place.*
Possible (C)	*It is quite possible that this event will occur again at some time e.g. 1 in 2 years. Poor supervision or defeatable controls are in place.*
Unlikely (D)	*There is a slight chance of this event occurring again e.g. 1 in 5 years. Defined safe systems of work are in place with only occasional exposure.*
Rare (E)	*This event may occur again but only in exceptional circumstances e.g. 1 in 10 years. The activity is adequately controlled e.g. effective policy, training, supervision, etc, in place.*

5. Consider and identify any uncertainties in the estimates

In estimation phase of likelihood and consequence, there will be always uncertainties. It is always an advantage to define and monitor as well as pay attention to these uncertainties any growth within risk level, although it may not be essential sometimes to react against these uncertainties. To be informed about the

[36] Australian Goverment – Department of Defence (2009), (Consulted on 07.10.2009)
[37] Worcestershire Health Services/UK (2009), (Consulted on 07.10.2009)

uncertainties let organisations to take actions as early and quickly as possible against these uncertainties when they become risks and threat the objectives of the organisation.

Once risk analysing concept is explained, the next step will be the introduction of how risk is analysed. Generally there are three types of risk analysis used and the type of the analysis method which will be chosen depends on the field and type of risk which is analysed.

"Types of Analysis" [38]

1. *qualitative*
2. *quantitative*
3. *semi-quantitative*

1. Qualitative Risk Analysis

This is the method which is used more than other risk analysis techniques in practice due to its features of readily intelligibility and simplicity.

There are some advantages and disadvantages of this method, for example as it is mentioned before, it is easy to understand and simple to use. Conversely, it is extremely subjective compare to quantitative method which aims to analyse risks by using numerical and tangible as well as mathematical assessments. It may affect the correctness of the analysed risk due to the fact of being subjective and intuitional.

Methods for qualitative risk analysis include:[39]

- *Brainstorming*
- *Evaluation using multi-disciplinary groups*
- *Specialist and expert judgement*
- *Structured interviews and/or questionnaires*
- *Word picture descriptors and risk categories*
- *…*

[38] Global Risk Alliance Pty. Ltd. jointly with NSW Department of State and Regional Development (2005), p.32
[39] Global Risk Alliance Pty. Ltd. jointly with NSW Department of State and Regional Development (2005), p.32

2. Quantitative Risk Analysis

The quantitative risk analysis can be defined from the engineering point of view as follows: *"QRA (Quantitative Risk Assessment) is a mathematical approach to engineers to predict the risks of accidents and give guidance on appropriate means of minimizing them. Nevertheless, while it uses scientific methods and verifiable data, QRA is a rather immature and highly judgmental technique, and it results have a large degree of uncertainty. Despite this, many branches of engineering have found that QRA can give useful guidance".*[40]

Moreover, another glance at quantitative risk analysis from project management thus and so:[41] The quantitative risk analysis more concentrates on the implementation of safety measures that have been established, in order to protect the project against all defined risk. By utilising a quantitative method, an organisation is capable of making a very precise analytical interpretation which can obviously point out the risk-resolving measures that have been most well-suited to different project needs. This advantage enables the quantitative approach to be used and preferred by many project management teams since risk assessments can be understandably determined in empirical manners like percentages or probability charts, since it underscores applying tools like metrics.

In addition to above-mentioned aspects, we can conclude this approach according to Prof. Modarres:[42] According to his comments in his book which is called Risk Analysis in Engineering, Techniques, tools and trends; Lately the usage of quantitative risk analysis has been regularly rising, mainly because of the availability of quantitative techniques, tools as well as methods, and secondly we are able to make quantitative estimation of adverse events and scenarios in complex systems from limited data. Nevertheless due to the quantitative risk analysis' complexity, expensiveness and time-consuming, it is not recommended to use this analysis for large scope risk analysis and further the usage of it is limited for these kind of analysis.

3. Semi-quantitative Risk Analysis

This approach is a kind of mixture of both methods which are introduced above. Hence, one of the semi-quantitative risk analysis techniques is risk ranking that

[40] Jason Batman (2009), p.1
[41] Cf: Preetam Kaushik (2009), (Consulted on 15.08.2009)
[42] Cf: Prof. Mohammad Modarres (2006), p. 6

includes the identification of hazardous events that could occur at a facility, quantification of the consequences of those events, and the estimation of relative probability of occurrence of each event.

The idea of the method is defined as follows by its own inventors whose invention has been patented in the name of them:[43] *"A semi-quantitative analysis on the risk management process increases the possibility of performing an accurate risks comparison, making easier the identification of which risks shall be prioritised and shall receive the greatest mitigation efforts. Specifically, the semi-quantitative risk analysis enables an improved risks comparison for evaluating the consequences of each risk considering its impacts on the project's Net Present Value (NPV), reflecting the project's cash flow at different times. The use of such method makes the prioritization process more efficient, helping the managers and other personnel involved on the process to focus their efforts to the most critical risks for the project's success. In this sense, the risk management process becomes more efficient and better able to provide better support to the project decision makers".*

In sum, the risk analysing concept has been comprehensively explained so far, once the risks, residual risks, potential opportunities and threats which may convert a possible risk in course of time, are properly and precisely analysed, the next step will be the evaluation step of all these matters which have been named above as risks, residual risks, threats and opportunities. The risk and every issue related risk will be broadly evaluated in the following chapter.

2.6.5 Step 5: Evaluate the Risks

After risk analysing step is completed, it is then vital to evaluate risks by comparing the estimated risks against risk criteria which the organisation has established before. The aim of this step is to determine the significance of risks and decide on whether the acceptance of the risks or taking actions against risks in order to minimise them. It is therefore necessary for organisations to determine the level of risks which are either accepted or treated.

In brief, this is the step for organisations to decide whether a risk should be accepted or needed treatment. Hence, obtaining the prioritised list of risks should be targeted as a result of the evaluation step.

[43] FreshPatents.com, (Consulted on 15.08.2009)

Risk Acceptance

"Low or tolerable risks may be accepted. "Acceptable" means the business chooses to 'accept' that the risks 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. This is also known as ALARP (as low as reasonably practicable).

A risk may be accepted for the following reasons:

- *The cost of treatment far exceeds the benefit, so that acceptance is the only option (applies particularly to lower ranked risks)*
- *The level of 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 justified*
- *The risk is such that there is no treatment available, for example the risk that the business may suffer storm damage.*
- ..."[44]

At the same time, in some cases cost of reducing a potential risk can be higher than the expected one. That is why; doing nothing against these risks makes more sense in terms of business. Table 3 illustrates the risk level with management action and acceptability.

Risk level	***Acceptability***	***Management Action***
Low (L)	*Acceptable with existing controls*	*- Ongoing monitoring and review*
Moderate (M)	*Acceptable with existing controls*	*- Ongoing monitoring and review* *- Assign management responsibility for monitoring*

Table 3 continues on following page.

[44] Global Risk Alliance Pty. Ltd. jointly with NSW Department of State and Regional Development (2005), p.33

Table 3continues as follows.

High (H)	*Unacceptable with existing controls*	*- Select and implement treatment option* *- Assign management responsibility for monitoring* *- Oversight of treatment by senior management*
Extreme (E)	*Unacceptable with existing controls*	*- Select and implement treatment option immediately* *- Assign management responsibility for treatment* *- Supervision of treatment by senior management*

Table 3 - Risk level with management action and acceptability[45]

There are some other tools which help organisations to evaluate risks, for example the risk map. The organisations can draw on a risk map the significance and likelihood of risk occurring. The risks are categorised and ranked from one to ten on a scale. Ten points symbolises the major importance to organisation, when a risk is rated ten. Conversely, one represents the least importance. The map lets organisations to imagine the risks and relations with each other and determine their size. It also structures a plan for determination of what type of controls should be taken in order to reduce risks.

Finally, in order to embed the risk evaluation step, an example concerning risk acceptance and its further discussions can be mentioned as follows:

"Example – risk acceptance" [46]

A newsagent identifies a risk of theft from her store. Existing controls include mirrors and the counter being close to the front of the shop. In analysing the risk she identifies that an additional way of reducing the residual risk is to install a security camera and/or security alarms, which will alert staff, if an item has been stolen. The cost of these treatment strategies is over $5000. The owner expects that the annual value of items that might be stolen would be less that $1000. So she decides to accept this risk.

[45] Queensland Government – Environment and Resource Management (2008), p.10
[46] Global Risk Alliance Pty. Ltd. jointly with NSW Department of State and Regional Development (2005), p.33

Discussion

Although the newsagent has decided to accept the risk, she should continue to regularly monitor the loss from the store. The majority of items sold are relatively inexpensive; however, should the store decide to stock larger items, or if the security of staff is compromised, or if the amount of loss increases above an acceptable level, or the cost of the treatment significantly reduces, the newsagent should reconsider the additional options for increasing security at the store.

2.6.6 Step 6: Treat the Risks

Before risks are treated, the question of whether risk treatment is necessary or not is arisen within the evaluation step above.

According to the answer of this question, in other words if the answer will be “YES”, then organisations take the next step so-called the risk treatment that will be explained within this chapter in detail. Conversely, if the answer of the question will be “NO”, then organisations would possibly keep monitoring risks without doing anything against them.

The aim of this step is to determine the treatment options or how to treat to risks which are classified and considered unacceptable or intolerable within the risk evaluation step. It should aim to increase the impact of a positive risk as well. The choosing criteria of the possible treatment option are that it should be the most appropriate and feasible/applicable one in terms of cost-effectiveness and benefit. Hence, the objective of risk treatment stage is to lessen the level of risk to an acceptable level or as low as tolerably practicable. Figure 6 demonstrates the risk treating process which is modified from AS/NZS 4360:2004.

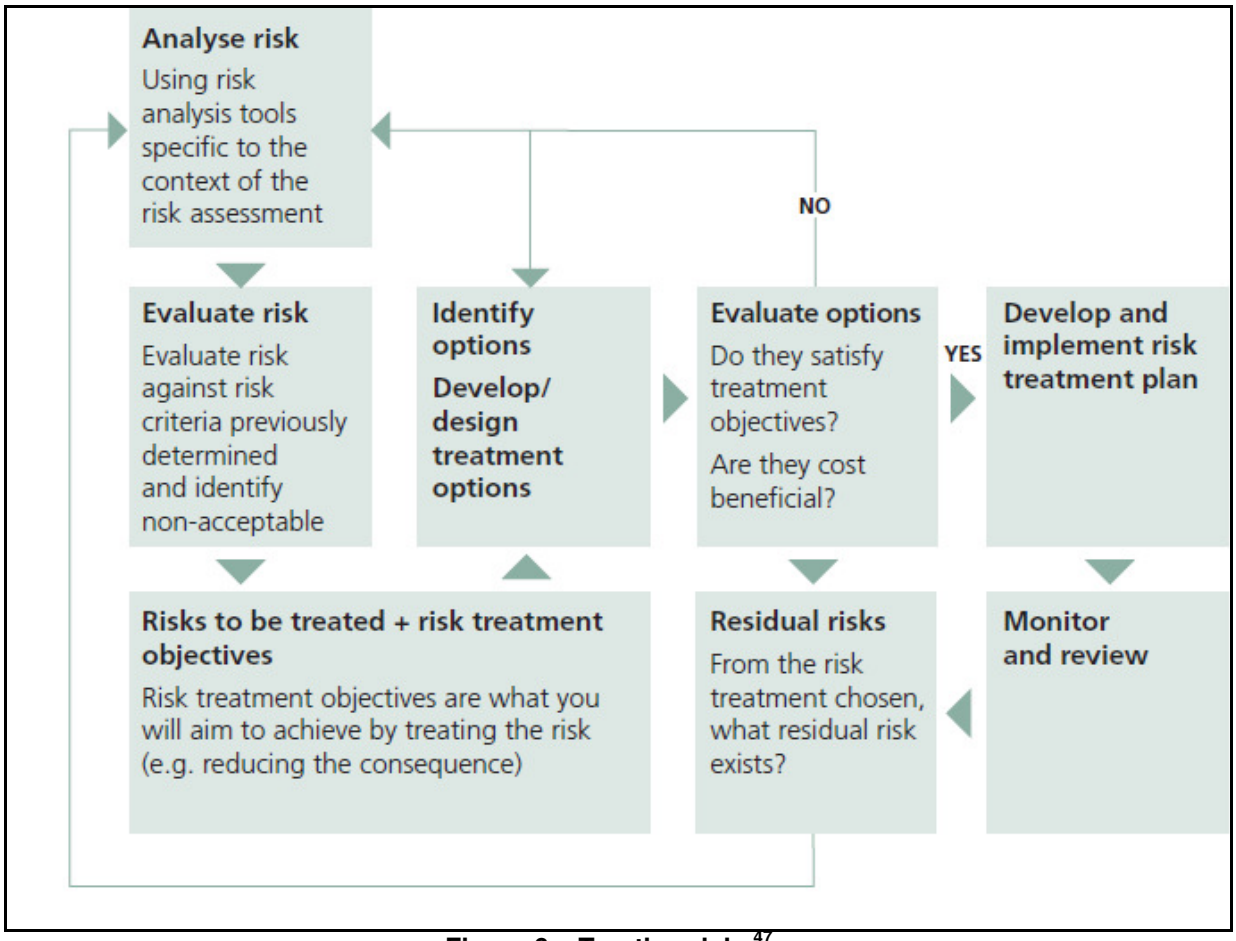


Figure 6 – Treating risks[47]

It is vital for organisations to know the root cause of a risk, as well as how the risk is arisen, before organisations start to treat a risk effectively. Thus, an example and its further discussions can be introduced here in order to clearly understand finding out the root cause of a risk, before risk treatment options are explained broadly.

"Example – treating the root cause" [48]

The business owner of a mechanical repair shop employing five staff is concerned that his business is constantly running behind time. He has recently received multiple complaints from clients. His head mechanic cannot provide an adequate reason for this fall in productivity. He mentions that a new employee who has only been working for the firm for five weeks may be the reason. This new employee orders the supplies. The head mechanic speaks to this new staff member on a number of occasions about his performance and tells him to improve it. The delays continue and the new employee is asked to leave.

[47] Global Risk Alliance Pty. Ltd. jointly with NSW Department of State and Regional Development (2005), p.34
[48] Global Risk Alliance Pty. Ltd. jointly with NSW Department of State and Regional Development (2005), p.35

Despite this action the delays in productivity continue. After some weeks, the business owner decides to close the shop for half a day and discuss the problem with his team. During discussion, it is revealed that there was a problem with the responsiveness of a new supplier. Although most staff had noticed this, each had considered the issue to be a 'once- off' and had not shared the information with the rest of the team.

Discussion

In this situation the root cause of the issue had not been identified in the first instance and so the risk issue was not effectively managed. Had the business owner or his senior staff member spent the time better understanding the issue at hand, the real cause of the problem may have been identified much earlier. The result would have been to retain the employee and not expose the business to risk of a claim for unfair dismissal, to manage the supply company in a more professional manner and to minimise impact on client satisfaction and therefore business reputation.

Once the aim and objective of risk treating as well as an overview regarding risk treating has been told, it is then necessary to look deeper through the risk treatment strategies. Some authors and risk management institutes name it as risk treatment options. There can be found out various classifications of risk treatment strategies (options) which are introduced by different authors or risk management institutions.

It would be very useful to utilize different point of views from different perspectives and gather them to determine the most appropriate risk treatment strategies. Therefore, while utilizing and mixing different perspectives together for the determination, it would be the best way to structure the risk treatment options according to AS/NZS 4360:2004 which has been internationally recognised the better risk management standard in practice.

Options/Strategies for risk treatment

There are basically five risk treatment options defined by AS/NZS 4360 which are used for minimising the negative risks or enhancing the maximisation of the impact of positive risks. Besides, some authors classify only four of them. Nevertheless, they all point out more or less the same understanding. The five risk treatment options will be introduced in this thesis with the support of examples for each of them which will be given right after the explanation of each option and aim to embed the concept of risk treatment options/strategies.

1. **Avoid the risk**

Avoiding the risk is about either stopping or not continuing the activity which causes risks or changing the plans and finding out an alternative and more acceptable activity to prevent risk arising. Organisations should only avoid risks they face, while either they do not have any risk control measures or the risk control measure they have cannot lessen risks in an acceptable and tolerable level.

The organisations should pay attention to the appropriateness and control of risk avoidance that they take. Because the activity that they take can possibly and effectively reduce a particular risk, even makes it zero, but might cause a risk arising in other department of the organisation or missed opportunities. For example, an organisation can avoid new technological investments and innovations. This strategy keeps specific risks away, even makes them zero. On the other hand, not investing new technologies or taking the advantage of innovations can affect the competitiveness of the organisation. After a while this organisation cannot compete with its rivals anymore. It might go to bankrupt in the end because of that fact.

"Example – avoiding the risk" [49]

A food retailer identifies that a particular item on the lunch menu contains an ingredient with a short shelf life. The retailer is concerned that the item may become unfit for consumption prior to sale. To avoid the risk of a food poisoning incident the item is removed from the menu.

2. **Change the likelihood of the occurrence**

This strategy targets to increase the likelihood of profitable results/outputs and lessen the possibility of losses.

This option can be achieved by taking some activities as follows:[50]

- *Audit and compliance programmes*
- *Inspection and process controls*
- *Preventative management*

[49] Global Risk Alliance Pty. Ltd. jointly with NSW Department of State and Regional Development (2005), p.35

[50] Queensland Government – Department of Education and Training (2006), (Consulted on 28.08.2009)

- *Structured training*
- *…*

"Example – changing the likelihood" [51]

A deli operator reduces the likelihood of a meat slicer blade injuring staff by ensuring that everyone has received early training on the use of the machine and that there are clear signs displayed demonstrating the correct techniques for its use and maintenance.

3. Change the consequences

This option aims to minimise the impact of risks and maximise the magnitude of gains by developing some consequence reduction/changing strategies. These strategies can contain risk recovery plans, crisis management, public relations, business continuity plans, emergency and contingency plans, and etc.

"Example – changing the consequences" [52]

A small pharmacy relies on a computer system to process and record prescriptions. The pharmacist backs up the computer system weekly and the back-up tapes are stored in a safe on-site. A risk analysis identifies that there is still a significant residual risk associated with this practice. The pharmacist then backs-up daily and stores the tapes off-site. Paper records are also now generated on a monthly basis and archived.

4. Share the risk

Some experts call this option as risk transferring. Both include the same context and understanding. It shortly means to share the responsibility of risk with another party or even simpler way to define it is to give risk to someone else.

The most well-known method to share or transfer the risk is insurance. The organisations can readily buy insurances against risks instead of taking actions to reduce the impact and consequences of them. For instance, purchasing a burglary

[51] Global Risk Alliance Pty. Ltd. jointly with NSW Department of State and Regional Development (2005), p.36
[52] Global Risk Alliance Pty. Ltd. jointly with NSW Department of State and Regional Development (2005), p.36

insurance for an automobile showroom instead of hiring security personnel or investing security equipments like security alarms, cameras and etc. It is also possible for organisations to transfer risk to the clients or other stakeholders by contractual arrangements, partnerships and business alliances. For example, adding a state/condition to the contract which is signed and accepted by both the client and organisation and it declares that the organisation does not take the responsibility of the related state, if it occurs somehow.

Thus the risk of this state/condition is transferred to client. Nevertheless, it is vital to know or to be aware of that the risk is not completely and hundred percent transferred to the third parties. In spite of some part of risks has been shared by another parties, the probability of a risk occurrence by a failure will always exist.

"Example – sharing the risk" [53]

A personal trainer currently has the professional indemnity insurance required to be a registered fitness professional in New South Wales (NSW). However, he has recently completed a course in child and adolescent fitness. His insurer indicates that the current insurance policy would not cover injury to individuals under the age of 14.

The personal trainer's insurance broker identifies an indemnity provider who will support the new requirement and provide the trainer with professional indemnity for provision of child fitness programs. The trainer has now shared or transferred his risk to the new insurance company.

5. Retain the risk

"This is the default choice for any risk management. You simply accept the risk as it is." [54]

Once strategies/options of risk treatment have been explained properly, it is time to introduce the risk treatment plan which demonstrates the preferred option for a defined risk treatment. Risk treatment plan should identify risk to be treated and level of risk, define the preferred treatment strategy, and specify the implementation schedule of the strategy. It should also determine the required resources and responsibilities (who will do what and by when) for making sure that the

[53] Global Risk Alliance Pty. Ltd. jointly with NSW Department of State and Regional Development (2005), p.36
[54] Douglas W. Hubbard (2009), Chapter 2, p.27

implementation of the risk treatment strategy is successfully done. The below-mentioned example and its further discussion allow readers to have a better understanding about risk treatment plan. Final documentation of risk treatment plan should also provide a budget, appropriate objectives, and milestones through the path to accomplish pre-determined objectives of organisation.

"Example – risk treatment plan" [55]

An event manager operating her own business in a regional area is contracted by a local council to assist in the management of a children's fair to be held in conjunction with the annual agricultural show.

The event manager organises a site assessment of the facility planned for the fair. A number of hazards and other general issues are identified, including the site's proximity to a busy road, absence of convenience facilities, a faulty drinking fountain and a damaged fence bordering a residential property next to the facility. The event manager, in conjunction with the council, develops a treatment plan that demonstrates how and when the identified risks will be addressed, the resources required and who will be responsible for ensuring the strategy is implemented. The treatment plan also identifies the need for subsequent site assessment to ensure that the identified risks have been successfully controlled to a level deemed appropriate by the organising committee.

Discussion

The risk treatment plan provides confidence to the council that there is a planned approach to addressing the identified risks. The document can also be used as a level of control and source of information when making decisions about signing off and resource allocation or approvals.

Another important issue to be mentioned regarding risk treatment is risk recovery which organisations should pay attention to obtain a comprehensively structured and prepared risk recovery plans. Some recovery plans will be briefly told in this thesis in order to conclude the risk treatment chapter.

[55] Global Risk Alliance Pty. Ltd. jointly with NSW Department of State and Regional Development (2005), p.37

- **Crisis or Emergency Management Planning**

Emergencies and crisis are unplanned and unexpected events which are occurred suddenly and may cause great damages and losses to the objectives of the business and organisation itself. Due to their unpredictability and immediacy, they have to be treated and managed according to short term plans. The natural catastrophes and disasters, a fire at a plant or an information security incident, hurricanes, and floods can be given as examples of crisis or emergencies.

Organisations always have to be aware of the emergencies and their possible impacts. They also have to assume and determine possible events (risks) which may cause a crisis or an emergency, before they occur. Training their staff for any crisis, informing each staff member about emergency response procedures and emergency contact details by arranging internal workshops can be introduced as effective applications of crisis and emergency management plans.

- **Business Continuity Planning**

The Public Safety Canada simply describes the business continuity planning on their webpage as follows: *"When critical services and products cannot be delivered, consequences can be severe. A Business Continuity Plan is a tool that allows institutions to not only to moderate risk, but also continuously deliver products and services despite disruption. A business continuity plan enables critical services or products to be continually delivered to clients. Instead of focusing on resuming a business after critical operations have ceased, or recovering after a disaster, a business continuity plan endeavours to ensure that critical operations continue to be available".*[56]

As a conclusion, business continuity is the ability to keep serving your duties and distributing your products to your customers, no matter what happens to your organisation.

- **Contingency planning**

Contingency plans can be the combination of a crisis/emergency management planning and a business continuity planning.

[56] Public Safety Canada (2009), (Consulted on 19.08.2009)

"They are sometimes known as "Back-up plans", "Worst-case scenario plans" or "Plan B". They are required to help governments, businesses or individuals to recover from serious incidents in the minimum time with minimum cost and disruption".[57]

An example regarding contingency planning would help to readers to embed the concept and the importance of contingency plans.

"Example – contingency planning" [58]

The senior accountant in a small accountancy firm travelling interstate has her laptop stolen from a restaurant where she is conducting a dinner meeting with clients. The laptop contains nearly four weeks of data that had not been backed up. This is significant loss of a large amount of personal information regarding clients and business opportunities. In addition to this loss, the accountant is now without use of a laptop and still has much client work to conduct.

Discussion

As a result of this loss the accountancy firm decides to conduct a contingency planning exercise, where the key business processes for the business are mapped and contingency plan is developed in the event that any of these processes fail. For example, the firm recognizes that the use of laptops by accounting staff is critical, as is the information the laptops contain. The contingency plan lists the warranty and insurance details of the asset, provides instructions on how to report the loss of the laptop and how to expedite replacement. It also provides instruction on how to access the software programs necessary for a new laptop to become functional as well as backed-up data. In addition to the contingency plan, the firm recognizes the lack of process and protocol in place for protection of data while staff is mobile and addresses this accordingly.

2.6.7 Step 7: Monitoring and Review

This is the last and one of the most important steps of entire risk management process. It is also a supplementary step like the first step and should be as important

[57] Wikipedia (2009), (Consulted on 20.08.2009)
[58] Global Risk Alliance Pty. Ltd. jointly with NSW Department of State and Regional Development (2005), p.38

as the first step of risk management process so-called Stakeholder Dialogue/Communication – Consultation.

Those two steps should be applied throughout the whole process due to risk management process should go on continually and these steps are the integral steps of entire risk management process. Furthermore, risks, organisation itself, changes in the organisation and environment in which the organisation operates are dynamic elements which have be periodically monitored, communicated as well as consulted by a well-trained risk management team as well as all associated people with risk management process. The risk management process and risk monitoring step therefore have to be repeated and updated regularly.

It should be known that only some risks are static. In order to achieve an effective risk management, organisations should ensure that all risks that an organisation encounters, namely the static and dynamic risks are properly identified, assessed and the implementation of all appropriate response procedures and controls are in place and executed correctly. This effective risk management can only be provided, if risks are periodically, the best case monthly or at least annually monitored and reviewed by risk management team with the supervision of board of directors.

2.7 Risk Management – Crisis Management – Safety Management

It is necessary to mention about brief descriptions and give an overview of Risk, Crisis and Safety Management as well as the major differences between all those management disciplines before we start to investigate deeper about Operational Risk Management in the next chapter. Because, it is still an open and unclear question for readers and industrial experts, what differs the risk management than the others and what the borders of all those management disciplines.

Although all those concepts are somehow related to each other, it would be helpful to enlighten above-mentioned questions for readers and industrial experts in order to let them know major differences among all those management concepts. Because a lot of industrial practitioners still do not know exactly what risk management, crisis management or safety management is. They suppose that all those concepts deal with the same problems that they encounter or they have the same approaches or understandings to solve problems. Therefore it would be vital to clearly and briefly define all of them and their paths to act against problems.

Despite several and broadly definitions of Risk Management that have been done in the beginning of this thesis, one of Risk Management's descriptions has been made by Accenture as follows which simplifies and makes the content of risk management clear for better understanding: "*Risk management is the process of identifying, categorising, measuring, monitoring and mitigating risks in an organization".*[59]

On the other hand, crisis management is a relatively new management approach. The definition of crisis management and the difference between Risk Management have been made as follows:[60] *"Crisis management is the process by which an organization deals with a major unpredictable event that threatens to harm the organization, its stakeholders, or the general public. In contrast to risk management, which involves assessing potential threats and finding the best ways to avoid those threats, crisis management involves dealing with threats after they have occurred. It is a discipline within the broader context of management consisting of skills and techniques required to identify, assess, understand, and cope with a serious situation, especially from the moment it first occurs to the point that recovery procedures start".*

Moreover, it would be helpful to announce and mention an example from the industry regarding crisis management and its applications right after its identification for embedding the concept of crisis management. The example is about a crisis that Pepsi Corporation has had in 1993 and how they could resolve the crisis:[61] The crisis began in 1993 with claims of syringes that have been found in diet Pepsi cans. Pepsi suggested markets and stores not to remove the product from their shelves while the situation and cans had been investigated. This led to an arrest, which Pepsi made public and afterwards they prepared the first video news release which showed their production processes to demonstrate and convince authorities that such tampering has been not possible within their plants.

In the second video it has been shown that the man has been arrested. Furthermore, the following video news release displayed the surveillance from an appropriate store where a woman was caught replicating the tampering incident. During the crisis, Pepsi has closely and publicly cooperated with FDA (The United States Food and Drug Administration). Besides Pepsi was entirely open with the public throughout, and they have kept informing their each employee about the details of crisis during the process. The Pepsi Corporation prepared some special campaigns that

[59] Accenture (2009), p.18
[60] Wikipedia (2009), (Consulted on 07.10.2009)
[61] Cf: RoadsideAmerica.com (2009), (Consulted on 07.10.2009)

contained coupons for further compensation, and thanked to the public for standing by corporation, after the crisis had been resolved. This example is a remarkable story which tells to organisations how to handle and deal with a crisis.

Finally, we describe the basics of safety management concept which has some similarities compare to risk management. Before the description of safety management is done, it would be helpful to identify what safety is. Once safety is defined correctly, it will be easy to execute it appropriately and efficiently. Hence, it will also be easy to understand how it relates to risk management as well as how it differs from risk management.

"Safety is the state in which the risk of harm to persons or of property damage is reduced to, and maintained at or below, an acceptable level through a continuing process of hazard identification and risk management.

The ICAO (International Civil Aviation Organisation) differentiates between safety programmes and safety management systems (SMS) as follows:

- *A **safety programme** is an integrated set of regulations and activities aimed at improving safety.*

- *A **safety management system (SMS)** is an organized approach to managing safety, including the necessary organizational structures, accountabilities, policies and procedures."* [62]

As it was said before that there are some similarities as well as dome differences between both management concepts. Although, it may not be commonly known that both management disciplines (Risk and Safety Management) do not generally work together, however they both aim the same goals and outcomes. The common goals of both are reduced losses and more efficient financing of these losses which lead to overall better operational efficiencies. This causes duplications or overlapping which are supposed to be inefficient and expensive. The operational effectiveness and cost reductions can be gained by integrating these combined concepts into a single discipline.

[62] The International Civil Aviation Organisation (2006), pp. 16-17

2.8 Summary

As a conclusion, full philosophy of risk management and its necessary components like risk management process, the definitions of crisis and safety managements besides risk management and major differences among all these management disciplines have been introduced so far by the aid of utilizing figures, tables, examples as short case studies and their further discussions. Once the clear understanding of entire risk management approach is achieved, it is going to be easy to understand and embed the next chapter of thesis which is the aimed topic of thesis, and called the introduction of operational risk management and furthermore the implementation of operational risk management.

The fully embedding of the risk management concept will allow readers and industrial practitioners to ensure that the determination of possible operational risks as well as response plans and procedures against these risks, determination of the responsibilities of operational risk management team are done. Hence, the identification of the departments of business in which possible operational risks will appear, briefly the implementation of the whole operational risk management concept will be managed and achieved appropriately and effectively.

3. OPERATIONAL RISK MANAGEMENT

Operational Risk Management which is a specialised form of traditional Risk Management will be comprehensively introduced in this chapter. First of all the basics and several descriptions of it will be made. After better understanding of its fundamentals is gained, it will be the time to look deeply through the challenges, tools, and methods of operational risk management, and how, where and by whom it can be put in practice. The following chapters will enlighten these issues which are actually related with and supposed to be a part of risk management concept that can be put in place practically within the industry and day-to-day business life.

3.1 Introduction to Operational Risk Management

Organisations have to focus on the effectiveness and efficiency of each aspects of their operations more than ever due to the challenges of today's business environment which create tougher competitions, market globalisation, increased client demands and expectations, higher flexibility, and specified high technologies. Today's way of doing business is complicated and will be more and more complicated in the future. Therefore, organisations have to pay more attention to the specialised concepts of risk management, like so-called Operational Risk Management (ORM) in order to reduce the possible operational related risks, and improve the operational performance in every branch of their business and thereby take the competitive advantage to lead the industry. They have to be aware of this specified field of risk management concept and invest more than ever for it; because Operational Risk Management itself, its implementation and the benefits of a well-implemented ORM on behalf of organisations are still neglected up to some extend by researches as well as industrial professionals.

The concept of Operational Risk Management has been introduced and significantly advanced in the early of 1990's when large losses occurred and big corporations failed due to these losses in terms of tons of dollars. Although, it was said above that the concept of ORM is neglected up to some levels by industrial professionals, and it is one of relatively young risk management discipline and it is on the way of evolving phase which becomes daily more and more important as the other management disciplines, e.g. quality, logistics or project management and etc. ORM is starting to become an accepted management discipline by industrial authorities.

3.2 Operational Risk

In order to have an idea about basics of ORM Concept, the identification of operational risk has to be introduced and understood firstly.

"An operational risk is a risk arising from execution of a company's business functions. The term operational risk is most commonly found in risk management programs of financial institutions that must organize their risk management program according to Basel II. In Basel II, risk management is divided into credit, market and operational risk management. In many cases, credit and market risks are handled through a company's financial department, whereas operational risk management is perhaps coordinated centrally but most commonly implemented in different operational units (e.g. the IT department takes care of information risks, the HR department takes care of personnel risks, etc).

The Basel Committee defines operational risk as: The risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events." [63]

It will be necessary and helpful to enhance the horizon of above-mentioned Basel Committee's risk management division and investigate more about the differences between different types of risks which affect organisation's chances for success as well as the reputation of organisation either negatively or positively when they occur. Afterwards, we will be able to understand what operational risk specifically is and what it deals with and further the differences between operational risk and the others.

"Operational risk includes legal risk, but excludes other risks that are not part of market or credit risk categories, such as strategic business risk and reputational risk. Strategic business risk is the risk of a loss from a poor strategic business decision, such as opening a store in the wrong location or producing a product no one would purchase. Reputational risk is the risk of a loss due to a change in a company's reputation or standing in the market or community. Yet, a significant operational risk loss or failure would definitely adversely impact the reputation of a company. Therefore, strategic/business, credit, market, liquidity, and operational risk all affect a company's reputation and by their nature create, increase, reduce, or alleviate reputational risk." [64]

[63] Wikipedia (2009), (Consulted on 29.08.2009)
[64] Kutenk (2009), (Consulted on 29.08.2009)

In addition to that, there are some another supportive point of views which explain what operational risk deals with:[65] *"According to Frame (2003), the operational risk is different from other types of risks as it deals with established processes rather than managing unknown circumstances. However, William et al (2006) points out that managing operational risks is not an easy undertaking because operational risks are interrelated in many complex ways. One operational risk can have impacts on other operational risks in the system".*

Therefore, it is a vital and must have duty for organisations to manage operational risks effectively in order to improve their operational performance and management efficiency to satisfy their customers, employees, shareholders, stakeholders, the authorities and other communities.

3.3 Operational Risk Management

Operational Risk Management (ORM) is described as follows by US Naval Safety Centre: *"ORM is a decision making tool - used by people at all levels to increase operational effectiveness by anticipating hazards and reducing the potential for loss, thereby increasing the probability of a successful mission."* [66]

The above-mentioned definition can be understood from the military point of view, but it is also correct and valid for the other risk management perspectives in which operational risks exist. In order to embed and broaden the horizon of ORM definition and before we would like to manage operational risks effectively, the questions of what we understand from operational risks or what considered as an operational risk should be enlightened and investigated deeply after the description of operational risk.

It was mentioned before that the Basel Committee classified risk management in three major categories, the market risk management, credit risk management and operational risk management. It is necessary to clearly understand the differences of different types of risks which are handled differently by various risk management perspectives in order to answer above-mentioned questions as well as broaden the ORM definition.

[65] Thitima Pitinanondha (2008), p.2
[66] US Naval Safety Center (2009), p.2

"The key difference between operational risk and all other types of risks is expectation. We expect market risk when we purchase an investment. We expect credit risk when we loan money to someone else. We do not expect a process or system to not work. We expect things to work. We do not expect things to go wrong. Operational risk is the risk of loss from something's unexpectedly going wrong. We do not want operational risk, although we are forced to live with it." [67]

Moreover, ORM has to manage and minimise potential losses effectively which are occurred due to operational risk. And if they occur, ORM has to reduce them to an acceptable level. *"Operational risk is typically associated with following types of potential loss:*[68]

- ***People.*** *Employees could intentionally or unintentionally make mistakes or fail to follow existing policies or procedures, resulting in losses.*
- ***Process.*** *Deficiencies in an existing procedure, or the absence of a procedure could result in losses.*
- ***Systems.*** *Automated processes and systems plus the underlying technology security or infrastructure could break down and cause losses.*
- ***External.*** *Third-party actions and other artificial or natural forces could create losses for a company."*

In addition to above-mentioned potential loss types, some examples can be given from day-to-day business life regarding above-mentioned issues. It is not hard to find out these kinds of examples from various operations. The samples are as follows:

- When a computer breaks down or is out of order in an office, then a day-work or even the entire work of which has been done by that computer is lost. We therefore have to pay overtime for catching up. This is a kind of operational risk and a potential loss afterwards which is associated with Systems.
- When a project manager estimates the task complexity of a certain project wrongly, then the project over-runs due to that underestimation. This failure outcomes some qualitative and quantitative consequences, e.g. loss of company's reputation because of not to accomplish the project on time as it has been scheduled before, or loss of money and so on. That is why; this is

[67] Kutenk (2009), (Consulted on 29.08.2009)
[68] Kutenk (2009), (Consulted on 30.08.2009)

also a kind of operational risk and a potential loss afterwards which is associated with People.

- When a subsidence of a building occurs or a damage of the factory building due to an earthquake, a tornado, or a flood, this is a kind of operational risk and a potential loss because of that risk which is associated with External, so-called Natural Catastrophes/Force.

On the other hand, the definition of an effective Operational Risk Management has been made by British Telecommunications as follows: *"…operate within a targeted level of risk parameters, and in full compliance with regulatory and corporate guidelines, aligned with business objectives, maximising operational performance while simultaneously minimising cost…"* [69]

To summarise the above-mentioned definitions by putting all aspects together from different point of views about Operational Risk Management, we can briefly explain it again as follows; Operational Risk Management is a decision-making tool which systematically helps to identify operational risks and benefits out of them as well as determine the best actions/reactions against any risky situation which is given. Hence, ORM is basically designed to minimise risks and maximise opportunities on behalf of organisations like the other risk management concepts, e.g. Supply Chain Risk Management, Enterprise Risk Management and etc. One of the key differences for ORM is that it is performed during operational uses.

3.4 The Elements and Principles of Operational Risk Management

When we talk about the elements and principles of Operational Risk Management, first of all it is necessary to mention the objectives of Operational Risk Management as basis which are related to traditional Risk Management approach. Therefore, the below-shown Figure 7 illustrates the objectives/goals of ORM process, while we name some of them as follows:

- Protecting people, equipment and other resources
- Making the most effective usage of above mentioned parameters
- Preventing incidents, qualitative and quantitative loses in terms of monetary, reputation as well as human lives.

[69] British Telecommunications (2005), p.2

- Achieving above mentioned gains by minimizing risks and maximizing opportunities
- Reducing costs and sticking to schedule
- Increasing the effectiveness of people, machines, and resources by the exact determination of how they can be used most efficiently as the fundamental objective of ORM as well as Risk Management.
- ...

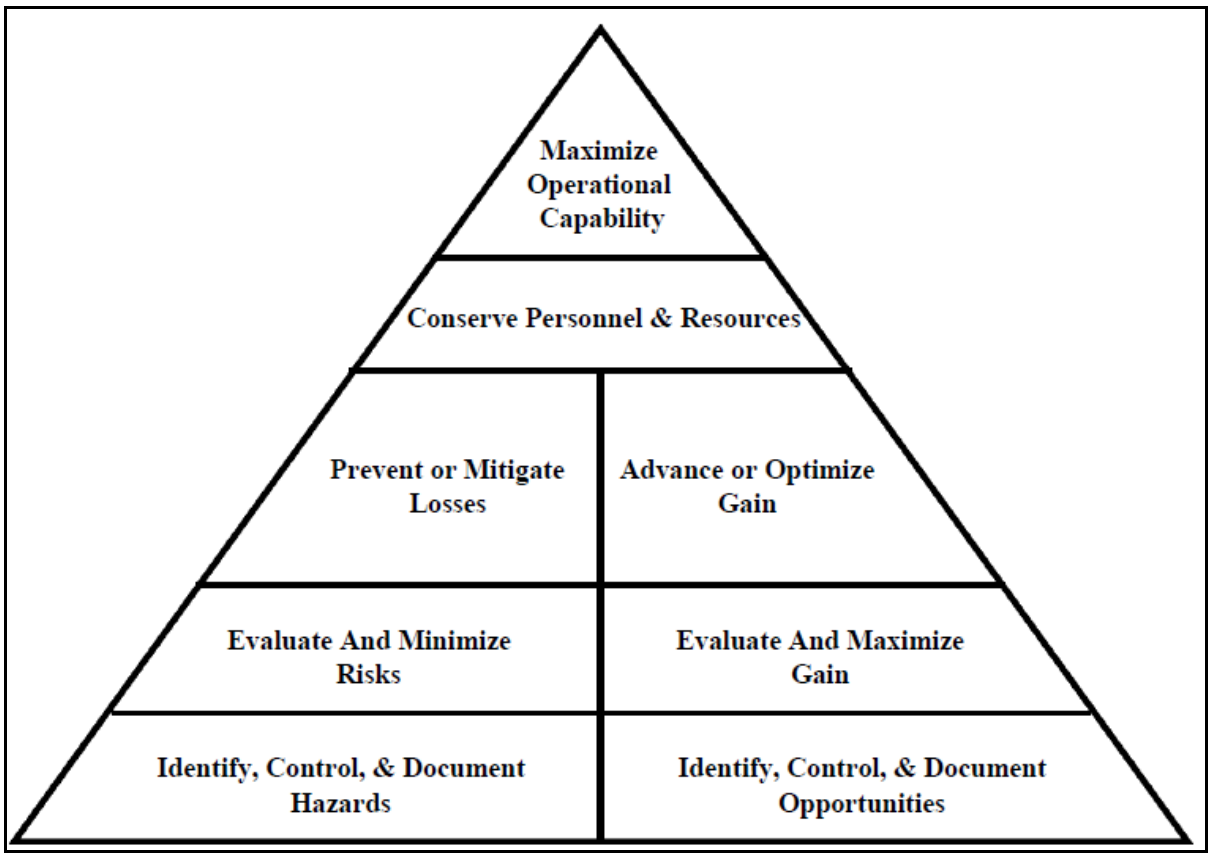


Figure 7 – Risk Management Goals[70]

After the goals and objectives of Operational Risk Management have been determined above, it is vital to set up the principles of ORM, before we announce the key elements of it. The goals, objectives, principles, and elements of ORM are aimed to be introduced broadly as a fundament for better understanding, and integrating the ORM Concept into day-to-day business life.

[70] Federal Aviataion Administration (FAA) System Safety Handbook, (2000), Chapter 15, p.3

"The U.S. Department of Defence summarizes the principles of ORM as follows:[71]

- *Accept risk when benefits outweigh the cost.*
- *Accept no unnecessary risk.*
- *Anticipate and manage risk by planning.*
- *Make risk decisions at the right level."*

Systems consist of certain goals, objectives, principles and elements. In this case, the system with its exact and pre-determined parameters which have been told above is named Operational Risk Management System. An ORM system can be defined as follows:[72] *"A management system for managing losses in operational processes based on leadership, planning and strategic alignment, implementation, monitoring and continuous improvement, training and performance appraisal, employee involvement and empowerment, and communication.*"

Once the system, specifically Operational Risk Management System has been identified, it is further required to state its elements and mention briefly about them. The elements of an Operational Risk Management Framework are stated as follows:[73]

- *Element 1: Leadership*
- *Element 2: Planning and strategic alignment*
- *Element 3: Implementation*
- *Element 4: Monitoring and continuous improvement*
- *Element 5: Training and performance appraisal*
- *Element 6: Employee involvement and empowerment*
- *Element 7: Communication*

3.4.1 Element 1: Leadership

One of the most impressive definitions about Leader and Leadership has been stated by The Drucker Foundation as follows: *"The only definition of a leader is someone who has followers."*[74]

---

[71] U.S Naval Safety Center (Consulted on 09.10.2009)
[72] Thitima Pitinanondha (2008), p.36
[73] Thitima Pitinanondha (2008), p.p. 36 - 40
[74] University of Exeter/UK, (Consulted on 09.10.2009)

Meanwhile, an efficient management system is directly related with the approach and role of the top management according to many management studies. It is the major duty of the top management to structure, implement and lead a long-term vision for the organisation. In addition, we can re-define the concept of leadership again as follows; the leadership is the ability of top management to lead the organisation to long-term business success.

The lack of Top Management Commitment before, during and after a risky situation can be a reason of Management System Failure. Therefore, strong commitment of top management is a must as it is also required for the other management disciplines' successes. It is vital for organisations for gaining the success of an effective Operational Risk Management as well as achieving the pre-determined short, mid and long-term organisational goals.

On the other hand, strong commitment from top management is not the only key success factor on the way of reaching organisational success. The properly and exactly determined vision and policy can be given as the supplementary motivators which can be used to perform the process. So, strong commitment, clear vision and policy are necessary and have to be combined for the success of an effective leadership as Jack Welch, the former Chairman and CEO of General Electric Co. said, *"Good business leaders create a vision, articulate the vision, passionately own the vision and relentlessly drive it to completion."* [75]

3.4.2 Element 2: Planning and Strategic Alignment

On the one hand, one of the most crucial and core processes of a system is planning which allows to identify and control the other processes readily within the system. On the other hand, strategic plan guides organisations through the way of accomplishing their objectives and goals. That is why; the main interest of organisations should be to ensure and provide the alignment of strategic planning with business strategies for gaining pre-determined goals as well as the chance of the organisation's success.

An Operational Risk Management Plan has to clarify the steps and patterns of how an ORM should be appropriately and properly established, implemented and managed along the organisation. As it has been stated in the very beginning of this thesis, the entire organisation from shop-floor to the top management should be concerned, aware and committed to the development stage of an ORM plan, while

[75] David Hakala (2008), (Consulted on 09.10.2009)

they are well-communicated each other with a transparent information policy at the all steps of development process. The commitment of all staff from downwards to upwards during the realisation and achievement steps of an ORM plan is recommended as a result of planning and strategic alignment.

3.4.3 Element 3: Implementation

Even though the implementation of an ORM will be broadly explained in the next chapters, it is necessary to mention briefly what an implementation of an ORM system means; *"The system is defined as the organisation structure, procedures, processes, and resources needed to implement the management (ISO8402 1994). After having the established plan, the organisation should put the plan into action. The implementation of an ORM system means to establish the system according to the plan which is based on the objectives, requirements, benefits and resources of the organisation."* [76]

3.4.4 Element 4: Monitoring and Continuous Improvement

As it has been pointed out in the previous chapter, while we were introducing the steps of Risk Management Process, it has been underlined that the monitoring step has to be kept during the whole process, because of risk's dynamism. Once again, risk is something dynamic which has to be checked out, reviewed and tracked periodically, e.g. weekly, monthly or at least annually. Hence, in terms of operations and operational point of view, monitoring should be a dynamic and systematic assessment which is utilized to identify the differences among the current performance and goals of the organisation.

An effectively gained Monitoring ensures continuous improvement on behalf of organisations by better understanding the root causes of risks and risky situations as well as regularly checking, reviewing entire process and specified fields in which are needed to be paid more attention, before a risky case appears or occurs. Furthermore, *"According to Flynn et al. (1994), monitoring and continuous improvement of the system can ensure all processes operate as expected."* [77] The establishment of an ORM system where the organisational targets that are described as key performance indicators, are met is the most important key player for monitoring and continuously improvement. Besides, the evaluation of continuous

[76] Thitima Pitinanondha (2008), p.38
[77] Thitima Pitinanondha (2008), p.38

improvement and standardisation of an ORM system can be executed by internal and external audits.

3.4.5 Element 5: Training and Performance Appraisal

"Training refers to the attainment of specific skills or knowledge that educates employees about how to perform their job activities, while education attempts to provide employees with general knowledge that can be applied in many different situations (Cherrington 1995)." [78]

It is necessary for organisations to train their staff in the right manner in order to obtain the full performance of them. Organisations and employees have mutual benefits from well-trained and educated personnel. As it was said above, organisations are aimed to get an efficient performance from their staff, while they are working for them. In addition, they need right people with right and sufficient skills to establish, implement and manage systems e.g. an Operational Risk Management System for the achievement of organisational success. On the other hand, staff members are needed to be trained and educated whenever they need in order to have a successful career for themselves as well as be felt that they are valuable and cared by their senior managers or bosses, while they are doing their jobs properly as how it is expected from them.

Meanwhile, good performance appraisals are needed for education and training operations. Organisations need performance analysis of their staff in order to check out and control the existing performance of them, whether they sufficiently perform or not, and what they additionally need to do their jobs in the right manner. Hence, performance assessment improves the communication between supervisor and employee, and it is an opportunity to collectively develop and set the goals of organisation, identifies the areas where training is needed.

3.4.6 Element 6: Employee Involvement and Empowerment

The employee involvement can be described as an environment in which staff members of an organisation are allowed to be involved the decision making and continuous improvement processes that affect what they do. In addition, it also deals with and determines the level of engagement of an employee within the

[78] Thitima Pitinanondha (2008), p.39

organisational and operational activities. Figure 8 illustrates Employee Involvement Diagram with its related elements.

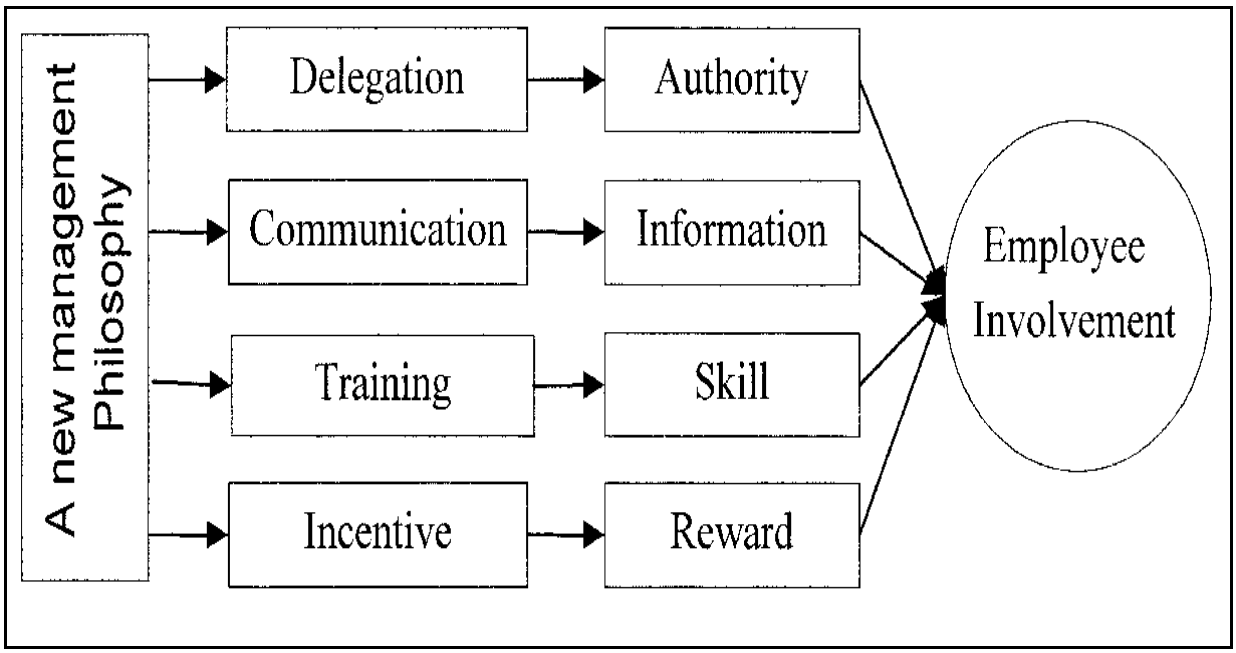


Figure 8 – Employee Involvement[79]

"Deming (1986) and Ishikawa (1985) stated that one way to motivate the employees at work is to let them accomplish things and see those things actually work." [80] In order to empower employees and let them to involve in decision making and continuous improvement processes is a strategic aspect of commitment and can include such methods as suggestions systems.[81]

- *Manufacturing cells*
- *Work teams*
- *Continuous improvement meetings*
- *Kaizen (Continuous Improvement) events*
- *Corrective action processes*
- *Periodic discussions with the supervisor*
- *…*

[79] Hongyi Sun, Ip Kee Hui, Agnes Y.K. Tam, Jan Frick (2000), p.p. 350-354
[80] Thitima Pitinanondha (2008), p.40
[81] Susan M. Heathfield, (Consulted on 14.10.2009)

Employee involvement and empowerment ensure highly motivated staff members with high performance. In order to manage the systems effectively, staff has to be empowered, trained, encouraged and supported by senior management to deal with and solve the problems that he/she encounters.

3.4.7 Element 7: Communication

It is vital for organisations to have an open and transparent communication process among all staff members throughout the organisation including top management. Once again, in order to obtain and implement an effective Operational Risk Management System, organisation has to communicate and consult each other during the entire ORM Process due to risk's dynamism, organisational and operational changes.

Risk management team's responsibilities and awareness should be established and properly communicated along the organisation. Everyone within the team should be correctly informed what he/she has to do and deal with. That requires two-way communication which means employees can easily communicate with their senior managers, when they need or have a problem to be solved. On the other hand, top management can also readily communicate and inform staff members, whenever they are needed. Two-way communication has to be ensured by organisations which aim to manage their ORM systems effectively and thereby reach their goals.

3.5 Summary

As the conclusion of chapter 3, the fundamentals, descriptions as well as elements and principles of ORM have been properly described and broadly mentioned so far for better understanding; once the concept and definitions of both Operational Risk and Operational Risk Management have been done and understood certainly, the next chapter will be the step by step explanation and comprehensively description of Operational Risk Management Implementation for integrating the entire conceptual basis as a whole into an organisation with its relevant steps.

4. IMPLEMENTATION OF OPERATIONAL RISK MANAGEMENT

Once Operational Risk Management concept is understood clearly, it is time to implement it. The implementation phase will be explained within the following chapters. Furthermore, we will broadly discuss about the hardness and challenges of an ORM Implementation and Culture that an organisation encounters, the methodologies and tools to implement an effective ORM, roles and responsibilities of an ORM team. In order to implement a successful ORM system into a business, organisations have to have an implementation plan which includes key plans, initiatives, and resource requirements as well as change management strategies. In addition, organisations have to support their implementation plans with the most appropriate technological instruments which are flexible and can be readily tailored and adopted to the changeable circumstances of operational risks and organisation itself.

4.1 Implementation Steps

Before we talk about the implementation steps of an effective Operational Risk Management, it would be helpful for better understanding of implementation concept to mention a *"proposed research model"* [82] which consists of the above-mentioned ORM elements that are supposed to be the factors that have an influence on ORM system implementation.

We should name these elements/factors in order to remain them. These are as follows: leadership; planning and strategic alignment; implementation; monitoring and continuous improvement; training and performance appraisal; employee involvement and empowerment; and communication. In addition, Figure 9 illustrates those elements which are split up into three major modules as follows: top management module; process management module; and human resource management module.

[82] Thitima Pitinanondha (2008), p.40

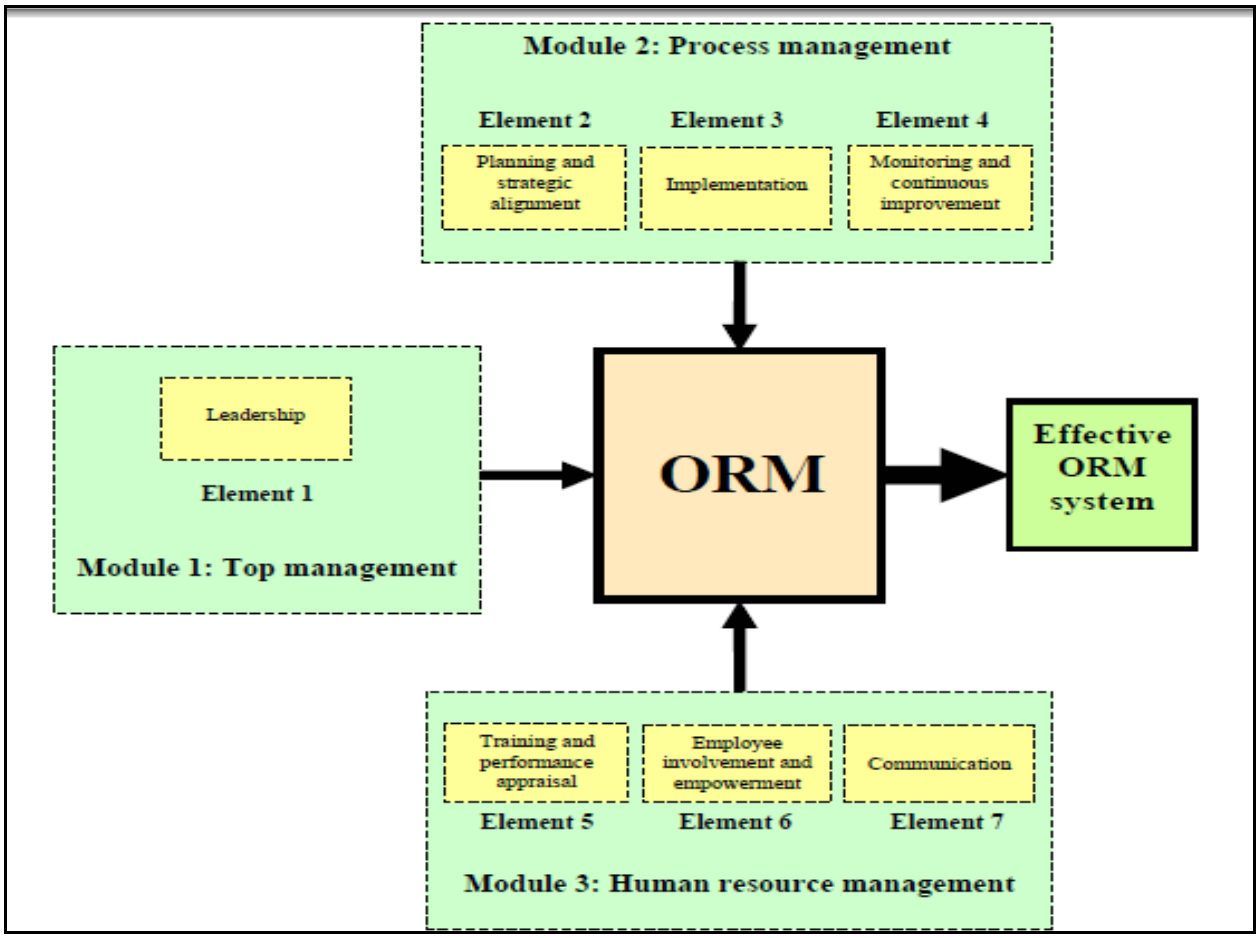


Figure 9 – the proposed ORM System Implementation Model[83]

4.1.1 Module 1: Top Management

This module explains and determines the duties and behaviours of top management during the implementation process of an effective Operational Risk Management System. Even though the roles and responsibilities of top management and risk management team will be explained broadly in the further chapters, it is vital to know that the leadership element plays a crucial role as a success factor which affects the entire system through the way of achieving pre-determined organisational objectives and goals.

4.1.2 Module 2: Process Management

It consists of three elements: planning and strategic alignment; implementation; and monitoring and continuous improvement as it was shown above on Figure 9. The process management module attends as the main processes of Operational Risk Management System which plan, implement and monitor the entire system.

[83] Thitima Pitinanondha (2008), p.42

4.1.3 Module 3: Human Resources Management

It is formed by three elements: training and performance appraisal; employee involvement and empowerment; and communication, as it was illustrated above on Figure 9. Human resources management is supposed to be the most important module for organisations, because it deals with human who are working as personnel in an organisation and support the organisation. Hence, it also plans, improves and executes the abilities of staff members and their potentials as human resources and thereby increases their contributions on behalf of organisations.

We can summarise this research model as follows; *"In this proposed model, the top management defines objectives, and sets direction and resources to achieve the organisation's goals. The process management module sets a plan aligned with business strategies, and executes and continuously improves operational performance, while human resource management module develops and motivates employees to utilise their potential to align with the organisation's objectives and delivers the results."*[84]

Once the proposed ORM system implementation model and its related modules were introduced, it is time to mention about the implementation steps of an effective ORM system. In this sense, the top ten requirements of Operational Risk Management which have been determined and classified by James Lam who is the founder and Vice Chairman of ERisk will be used and referred as the implementation steps of an effective ORM. According to James Lam;[85] *"Although operational risk is difficult to quantify, significant benefits can be gained from its successful management. The following ten steps to operational risk management can help increase the likelihood of achieving business objectives and reduce operational losses."*

These requirements as implementation steps are as follows:[86]

- *Step 1: Define it, and move on*
- *Step 2: Put someone in charge*
- *Step 3: Have a Letterman list*
- *Step 4: Know your losses*
- *Step 5: Have good brakes*
- *Step 6: Create one dashboard*

[84] Thitima Pitinanondha (2008), p.43
[85] James Lam (2001), (Consulted on 25.10.2009)
[86] James Lam (2001), (Consulted on 25.10.2009)

- *Step 7: Peel the onion*
- *Step 8: Break down the silos*
- *Step 9: Transfer risk, if the price is right*
- *Step 10: Balance the ying and the yang*

4.1.4 Step 1: Define it, and move on

It is a common and general approach to define an event or issue before starting up to deal with and work on it. In addition, it is even crucial to define that issue properly for a common and clear understanding by everyone else who are involved with this issue. In this sense, organisations have some problems to find out the correct and the best definition of operational risk. Thus, on the one hand they waste too much time to obtain the right definition; on the other hand, even though they find out the definition after spending too much time, the definitions of operational risk; operational risk management and etc. may not be understood in the same way by all employees within the organisation. In addition, this misunderstanding or not having the same approach about a certain issue among staff causes additional problems and even suddenly-appeared risks that occur within the further steps or during the implementation process.

The organisations should therefore standardise the definitions that they want all involved people to have a common understanding about what they deal with, before they move on. Once a certain matter is similarly and obviously understood, going forward for the implementation of it will be easier. Besides, James Lam also agrees with the idea that we mentioned above as follows;[87] *"Instead, a company should adopt a common definition, such as "risk of loss due to failures in people, processes and systems or an external event," or create a more tailored and workable definition, which can always be changed later on."*

4.1.5 Step 2: Put someone in charge

While Risk Management has been defined at the very beginning of this thesis, it has been referred at the end of true life story of The Albuquerque Accident of Ericsson that the related accident dramatically taught Ericssson that they had to change their risk management mentality. After the accident, Ericssson's risk management philosophy has been changed and they have decided that "everyone is risk manager" within the organisation.

[87] James Lam (2001), (Consulted on 25.10.2009)

Ericsson's new risk management philosophy should also be valid for operational risk management for all organisations especially nowadays business environment whose complexity is increasing daily and in which the competition is getting tougher day by day. Organisations have to reduce expected and unexpected operational failures which are caused by people, processes, systems or external events by tracking and checking them out periodically by some specialised and well-trained person who is put in charge of doing this specific job, even though operational risk management is everyone's job. In order to achieve the philosophy of everyone is risk manager as well as make the entire organisation aware of that managing all kind of risks including operational risks is one of their job to do, the traditional and operational risk management trainings and workshops have to be especially provided to project and line managers as well as the entire organisation.

In this sense, an operational risk officer who is in charge of executing all operational risks' operations has to be determined. Afterwards, his or her duties have to be determined clearly. He/she has to be responsible for defining, implementing and developing the infrastructure, framework, policies, and processes of an effective ORM system as well as gathering and integrating all these activities into an enterprise risk management program. For example, first of all, as we mentioned in the previous step above, he/she should determine the common definitions for operational risk; develop and facilitate the implementation of common risk management tools such as risk maps, self-assessment programs, and loss event databases; and develop measurement models and etc. Consequently, operational risk officer has to take the overall responsibility for all operational risk management operations with their positive or negative outcomes. In addition, the roles and responsibilities of all operational risk management team will be comprehensively told within the further chapters.

4.1.6 Step 3: Have a Letterman List

"A common complaint from board members and senior management is that they get too much data and not enough information. Every company should identify the top ten risks it faces, using self assessments, risk maps and operational risk metrics. In many cases, these risks can account for over 80 percent of potential losses. Further, each risk should be tested against historical losses and incidents to ensure quality." [88]

[88] James Lam (2001), (Consulted on 25.10.2009)

As James Lam stated above, we have also identified the top ten risks for global business by the aid The 2009 Ernst & Young Business Risk Report in the very beginning of this thesis. The definition of all types of risks that an enterprise encounters plays a vital role for gaining organisational success. The operational risk officer also plays a crucial role for ensuring that all risks including operational risks are clearly and properly classified and the top ten of them are obviously determined and identified.

Moreover, Operational Risk Officer has to additionally prepare an operational risk progress report which contains the list of top ten risks and their controlling actions. He/she should further introduce a systematic method which is supported by brainstorming techniques as well as checklists that are put in practice by arranging internal workshops and trainings. Thus he/she enables the rest of operational risk team and affected people to be involved into the risk identification sessions for each project

4.1.7 Step 4: Know your losses

It is obviously clear that knowing the losses or being aware of losses is a plus for organisations, and it is further a key challenge to quantify the losses in implementing the framework of Operational Risk Management. Moreover, before trying to assign a number to a particular operational risk, we should think about how we define and group operational losses which might arise from that operational risk.

Operational losses should be defined as definite as possible. In this sense, the following definition of operational risk losses can be used:[89] *"The direct loss, including external direct or write-down involved in the resolution of the operational loss event, net of recoveries."* If we summarise what we have told above, the losses include payments to third parties, write-downs, resolutions, and cost-to-fix which are included only the external payments that are directly connected to incidents, such as consultancy costs or hiring temporary staff. Conversely, losses do not include the cost of controls, preventive actions, and quality assurance. In addition to that, losses do not usually include investment in upgrades or new systems and processes.

[89] Douglas G. Hoffman, (2002), p.51

Nevertheless, Table 4 represents seven loss event types according to the new Basel Capital Accord.

Event types and descriptions according to Basel II	
Event Type	**Definition and Examples**
Internal Fraud	Losses caused by acts of a type intended to defraud, misappropriate property, or circumvent regulations, the law, or company policy. For example, intentional misreporting of positions, employee theft, and insider trading on an employee's own account.
External Fraud	Losses caused by acts of a third party of a type intended to defraud, misappropriate property, or circumvent the law. For example, robbery, forgery, check kiting, and damage from computer hacking.
Employment Practices and Workplace Safety	Losses arising from acts inconsistent with employment, health, or safety laws or arrangements, from payment of personal injury claims, or from discrimination events. For example, violation of organised labour activities.
Clients, products, and business practices	Losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature of design of a product. For example, misuse of confidential customer information.

Table 4 continues on following page.

Table 4 continues as follows.

Damage to physical assets	Losses arising from loss or damage to physical assets from natural disaster or other events. For example, terrorism, vandalism, earthquakes, fire and floods.
Business disruption and system failures	Losses arising from disruption of business or system failures. For example, hard-ware and software failures, telecommunication problems, and utility outages.
Execution, delivery, and process management	Losses arising from failed transaction processing or process management, or from relations with trade counterparties and vendors, For example, data entry errors, collateral management failures, incomplete legal documentation, and unapproved access to client accounts.

Table 4 - Operational event types, their descriptions, and examples according to the new Basel Capital Accord[90]

By the way, it is recommended to establish and utilize a common loss event database as a tool for Operational Risk Management Implementation. In other words, an integrated ORM technology platform which is required in order to support the implementation of Operational Risk Management would be more effective, if it is supported by an integrated database. This database should also include the sources like legal data, fraud data, and etc. and uses like reporting, frequency/severity analysis and so on. Furthermore, Figure 10 illustrates this loss event database which is centralized and used as operational risk database.

[90] Cf: Michel Crouhy, Dan Galai, Robert Mark, (2006), pp.333 - 334

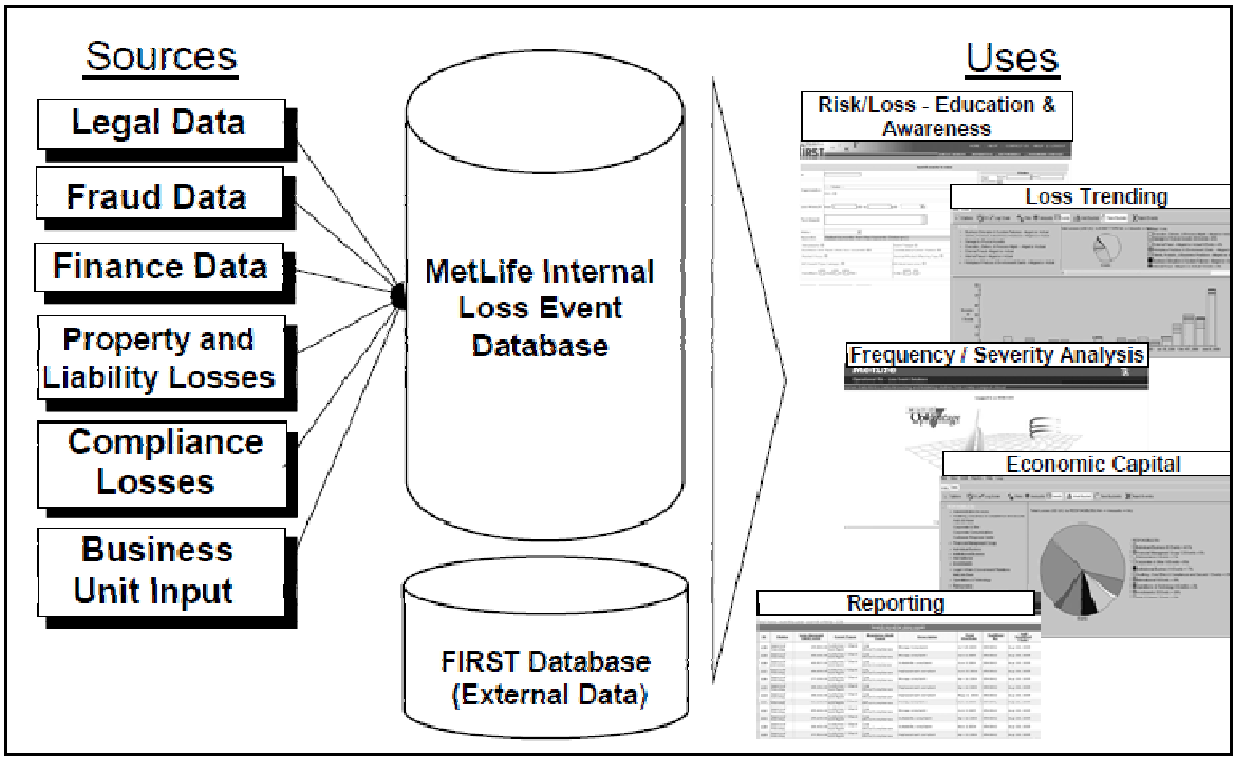


Figure 10 – Using Loss Event Data[91]

In sum, we have talked about operational risk losses from the financial point of view due to the losses are generally determined and quantified by financial indicators/terminations. In addition to this point of view, operational risk losses may also be market, credit, strategic, reputational, and even human lives' losses. Therefore, organisations have to pay more attention on every kind of operational risks and losses which are occurred by these operational risks as well as the other risk which we have named above.

4.1.8 Step 5: Have good brakes[92]

Despite the fact of having brakes or good brakes allow a car to slow down, it also makes the driver more confident and him/her feel safer. In addition, having good brakes let him/her to drive even faster, because the driver knows that he/she has good brakes, whenever he/she needs to. For instance, the race cars, especially a Formula 1 car have the best brakes and these best brakes make them the fastest cars of the world and give a huge confidence to their drivers, while they are on a race.

[91] Robert Semke (2006), p. 5
[92] Cf: James Lam (2001), (Consulted on 03.11.2009)

The interpretation of having good brakes from operational point of view is that having risk limits may also allow a business or an organisation's operations to slow down. So, risk limits are the good brakes of a business or an operation. More specifically having good brakes for operational risks mean setting performance goals and limits for each operational risk area, establishing, and implementing periodic review to make sure that appropriate decisions and actions are taken.

4.1.9 Step 6: Create one dashboard

James Lam has stated this step as a recommendation of developing a risk dashboard reporting in his report which has been called Operational Risk Management – Beyond the Compliance to Value Creation.[93] He mentioned within his report that due to the operational risks are distributed along the organisation, Operational Risk Management is everybody's job in this organisation, as we have also announced the same in step 2 (put someone in charge). In fact, an Operational Risk Management program should supply useful role-based risk dashboard information to different levels of the organisation.

In this sense, an integrated technology platform as such Figure 10 that we have introduced and illustrated above would broaden risk visibility and support business decisions by bringing together and delivering risk information to each group based on their specific needs. For instance, board reporting should concentrate on regulatory compliance, policy decisions, and exceptions, and major strategic investments, while management reporting should focus on key corporate and business unit objectives as well as day-to-day operations. In addition to that, operational risk metrics should be integrated into enterprise risk management reporting, or even better, a part of the total performance measurement of the organisation. Risk reporting should provide losses, incidents, and early warning signals, with key risk indicators which are measured against performance goals and limits.

4.1.10 Step 7: Peel the onion

Peel the onion stands for the identification, understanding and fixation of the essential sources/reasons for operational problems. As we have explained before, while risk management process has been introduced, risk quantification and reporting is not the only job to do for the organisational chance for success. First of all, organisations have to figure out the root causes of any kind of risks including

[93] Cf: James Lam (2007), p.10

operational risks that they encounter. Secondly, they have to define and understand all operational risks properly in order to take the most appropriate and cost-effective actions as a result to reduce them on an acceptable and tolerable level or fix them, if the fixation operation is necessary.

In sum, organisations have to peel the onion in order to be aware of what is going on within their organisation. Being aware of the root causes of any operational problem, specifically operational risks allow organisations to take the advantage of early detection of an arising trouble by regular monitoring and reviewing, taking the most suitable preventative precautions and even the quickest action against any incident, if it happens unpredictably. Last but not least, early detection and preventative actions are the best management strategies for operational risks.

4.1.11 Step 8: Break down the silos

According to Oxford English Dictionary;[94] the silo is a Spanish originated word, and the Greek form of it is “Siros”. Besides, the English definition of silo is that a silo is a tall tower or pit on a farm, used to store grain, or a pit or other airtight structure in which green crops are stored as silage. But in this case, a silo is a metaphor for an organisational unit that has its own management team, and is unaware of the interests, goals, and achievements of other groups of the organisation, as well as lacks of motivation, or desire to work with, or even communicate with other organisational units in an organisation.

We should broaden the horizon of the metaphoric definition of silo, further interpret as well as correlate it in accordance with Operational Risk Management Implementation. In this case, silos represent the organisational units, in other words the departments of an organisation. More specifically silos between line management and risk management teams/departments should be broken down. In addition to that, silos within the risk management team itself, for instance silos between audits and compliance units should have been broken down in order to get an effective Operational Risk Management System.

After breaking down the silos between units in an organisation, organisation works more efficiently, because every units of organisation communicate and inform each other about everything that is happening in the organisation. Besides, every unit would be concerned about the goals, interests and achievements of the other

[94] Cf: Oxford English Dictionary, Harvard Business Publishing (Consulted on 04.11.2009)

organisational units whom they cooperate with. All these achievements will let the enterprise to be an effective and successful organisation in its day-to-day operations. Moreover, the enterprise operational risk management program should be worked together with other organisational units, like quality management department, project management, and supply chain departments and etc.

4.1.12 Step 9: Transfer risk, if the price is right

Risk transfer, allocation as well as risk sharing are the same expressions which are used to be named this step. It would be useful here to define once again what risk transfer or allocation means.

Risk transferring or allocation simply means assigning risk to somebody else by contractual arrangements/subcontracting or buying insurance. In addition to broaden this definition;[95] organisations should transfer all undesirable risks, including operational risks, only if the risk transfer cost is lower than the cost of risk retention. Hence, an enterprise should rationalise its risk transfer activities in accordance with the use of derivatives, insurance and alternative risk transfer products.

In order to strengthen above-mentioned definition of risk transfer and what we understood the concept of risk transferring, it would be helpful to introduce a simple example about risk transfer. The example continues as follows:[96] it is time to expand risk transfer definition via a given example which includes a bit fun. The given task of project is to design a new piece of equipment which is going to be utilized to test water temperature and current flow in the ocean. There can be lots of operational risks which can be found out regarding this project. But the given risk which is a bit funny is following; the risk of a shark attack while the recently designed device is being tested in the ocean will cause an injury to the testers, resulting delay of the project as well as increased costs.

The possibilities to transfer, allocate and share the above-mentioned risk may be as follows:

- Have your manager do the testing (I cannot help the humour. Do you really mind?)

[95] Cf: James Lam (2001), (Consulted on 06.11.2009)
[96] Cf: Rita Mulcahy, (2003), pp.158 - 159

- Hire a shark expert to perform the testing (Some ideas can qualify in more than one option.)
- Outsource the testing to a more experienced company familiar with and experienced with the risks
- Purchase shark attack insurance (is there such a thing?)
- Purchase liability insurance

The given risk has been transferred to third parties or shared above by either signing contractual arrangements or purchasing insurance. In addition, the number of above named transferring possibilities can be readily increased by a brainstorming session which all project members will participate.

4.1.13 Step 10: Balance the ying and yang

Another metaphoric implementation step of Operational Risk Management is balancing the ying and the yang. Before the interpretation of metaphoric expression of ying and yang, it would be necessary to clarify the real definition and philosophical meaning of the ying and yang.

Figure 11 symbolises the ying and yang below. As it can be seen on the figure, the black coloured part of the symbol is representing “the ying”, and the white coloured side symbolises “the yang”. In addition to that;[97] according to the ancient Chinese inscriptions, the ying and yang readily are the descriptors of natural phenomena like weather conditions, especially the movement of the sun. Furthermore, there is sun light during the day which stands for the yang and a lack of sun light at night which symbolises the ying. According to the earliest comprehensive dictionary of Chinese, ying stands for “a closed door, darkness and the south bank of a river and the north side of a mountain”, and yang refers to “height, brightness and south side of a mountain”.

[97] Cf: Internet Encyclopaedia of Philosophy (2006), (Consulted on 07.11.2009)

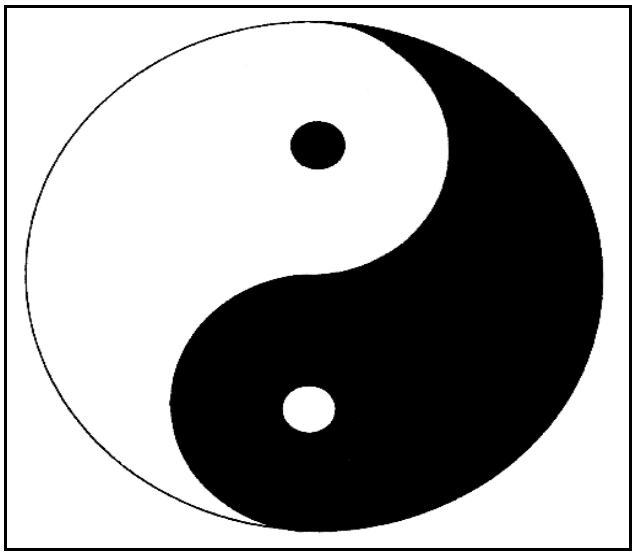


Figure 11 – The ying and yang[98]

We have explained the real meanings of the ying and yang so far, now it is time to interpret it in respect of Operational Risk Management implementation which will make it one of the important implementation steps of ORM. Because the success and realisation of the other implementation steps depend on the success and achievement of this step due to human factor that this step dominantly deals with. The metaphoric statement stands for the balance or harmony among the human factor and system itself. All systems, processes, policies or anything concerning business like in this sense, ORM is associated with human being.

There should be a harmony between the factors which are related to human being and systems, a maintained balance in the process which are gained by organisations in order to extract the most effective utilisation from all related factors. All resources, experiences and time should be allocated in order to obtain the full performance from all implementation steps. In addition to that, they should contribute each other and further supplement themselves as a whole like the ying and yang integrity in order to integrate ORM practices into day-to-day business operations and decisions.

On the other hand, according to James Lam;[99] *"Risk management is about people. It is critical to balance the hard side of risk management (e.g. policies, systems, limits) with the soft side (e.g. culture, values, incentives). An effective risk management program cannot be established with one and not the other."*

[98] Halfbit.org (Consulted on 07.11.2009)
[99] James Lam (2001), (Consulted on 07.11.2009)

Consequently, implementation of operational risk management and the comprehensive implementation steps have been explained step by step as yet. Organisations have to take into account the realisation of each implementation step as well as the entire implementation process. In order to attain an effectively implemented enterprise-wide operational risk management program, it is crucial to be aware of the importance of operational risk management concept as a whole, its objectives, goals, elements, and the implementation steps.

Once this conceptual implementation program is properly understood and successfully put in practice, it is time to have a deeper look through the challenges and difficulties to the implementation of effective Operational Risk Management into an enterprise. Because each organisation has some different responses to any changes within the organisation which will positively or negatively affect either only some departments' functions, or the entire business concept of the organisation. Into the following chapter, we shall further discuss how an effective ORM can be introduced and implemented into an organisation without facing or having any difficulties, and what the reactions against changes into an organisation are, as well as how these changes that an organisation faces can be efficiently managed by change management practices.

4.2 Challenges and Difficulties to the implementation of an effective Operational Risk Management

At the end of the previous chapter, we underscored that there is a resistance to any activities in an organisation which is associated with a change. In addition to that, there is a pressure for change which is tremendously and continually boosted by new trends and approaches of doing businesses, the stronger competitions, relationships of organisations with their clients, suppliers, and competitors as well as the changes within the organisation itself and thus organisational changes through mergers, acquisitions and etc. Hence, changes in an organisation sometimes can only affect some departments' positions and functionalities internally, like replacement of matrix organisational model with existing organisational management of an enterprise which will cause some changes within the organisation, but also affect the entire business environment of organisation externally, like mergers, acquisitions or any strategic decision which will be made by board members and will completely change the existing business sector of organisation, e.g. a manufacturing company decides to quit producing machineries and replaces its manufacturing business with hotel management business which are completely different sectors from each other.

In this sense, before we go further into the details of challenges and difficulties to the implementation of effective operational risk management, it would be necessary here to talk about change management, what it is, how it deals with integrating and embedding any changes successfully into an enterprise without facing any problems and the techniques of change management to manage the change associated with the introduction of the operational risk management program.

One of simple definitions of change management is as follows:[100] *"Change management is the process, tools and techniques to manage the people side of change to achieve the required business outcome. Change management incorporates the organisational tools that can be utilised to help individuals make successful personal transitions resulting in the adoption and realisation of change."*

Besides, change management is developed as a management discipline to contribute both the structure and required tools to make change real successfully on the technical and people side, as it is introduced on Table 5 below. In addition to change management tools which are underscored on Table 5, management support, open, and transparent communication among the personnel and executive officers are useful supporting techniques which are utilised to manage the change, while an effective operational risk management is aimed to be introduced and implemented into an organisation.

Discipline	***Process***	***Goal/Objective***	***Tools***
Change Management	** Planning for change* ** Managing change* ** Reinforcing change*	** To apply a systematic approach to helping the individuals impacted "the change" to be successful by building support* ** Addressing resistance and developing required knowledge and ability to implement the change (managing the "people" side of the change)*	** Individual change model* **Communications* ** Sponsorship* ** Coaching* ** Training* ** Resistance Management*

Table 5 - Change Management Discipline, Processes, Goals/Objectives, and Tools[101]

[100] Tim Creasey (2009), (Consulted on 10.11.2009)
[101] Tim Creasey (2009), (Consulted on 10.11.2009)

Once the definition, processes, goals and tools of change management are broadly introduced;[102] it is time to mention and look deeper through the most well-known change management model which has been created by McKinsey & Company's consultants whose names are Tom Peters and Robert Waterman and recognised as McKinsey's 7-S Model. The model is depicted on Figure 12. Moreover, the model primarily says that an organisation is not just all about structure, but consists of seven elements as shown on Figure 12. These seven elements are distinguished in hard and soft elements, so-called hard S's and soft S's. The hard elements are determined with dark blue colours on the figure, and the soft elements are symbolised by light blue colours.

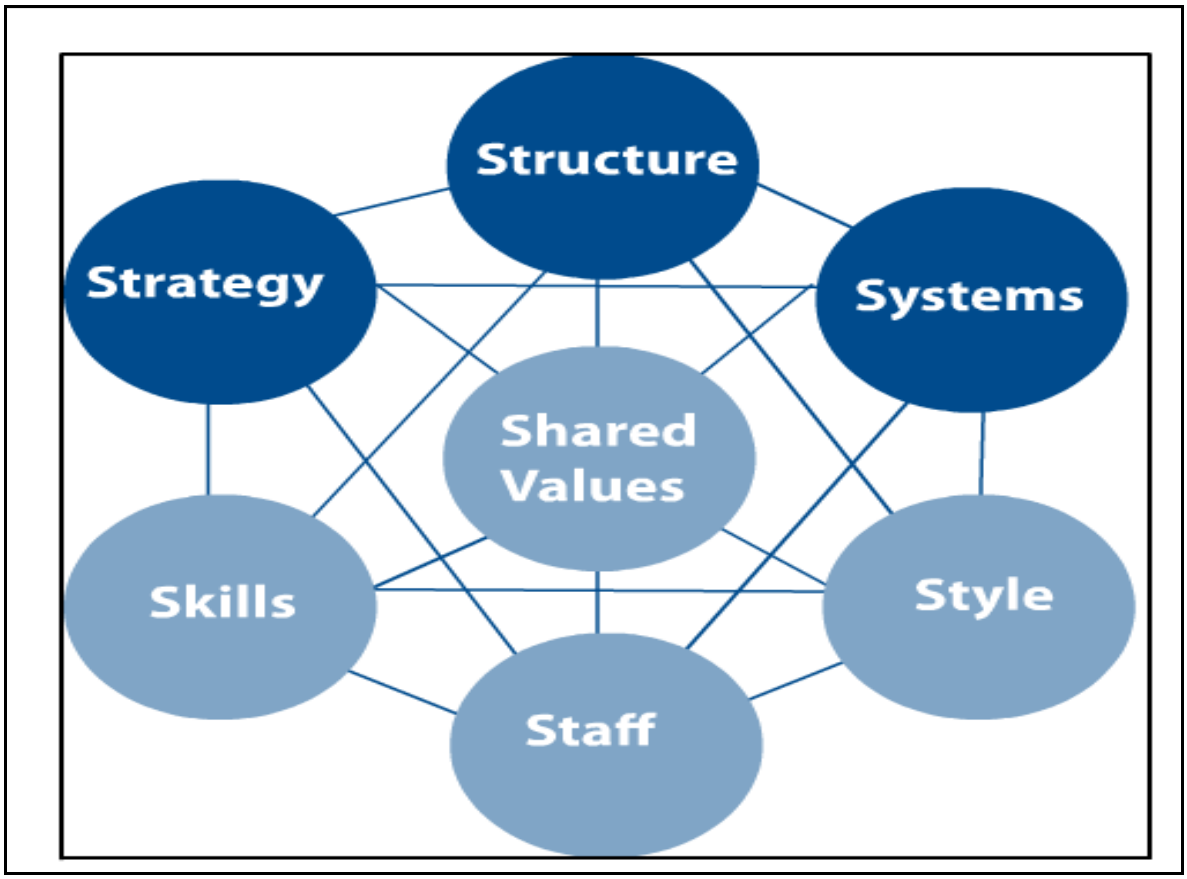


Figure 12 - McKinsey's 7-S Model[103]

On the one hand, the hard elements (dark blue coloured) are feasible and simple to define. They can be seen and found out in the strategy statements, corporate plans, organisational charts and other documents. On the other hand, the soft elements (light blue coloured) are not readily practicable. It is hard to describe them since capabilities, values, and elements of corporate culture are continually developing and changing. Therefore, they have a great impact on the hard elements, strategies and

[102] Cf: Avner Barnea (2008), pp. 51-52
[103] Avner Barnea (2008), pp. 51-52

systems of the organisation, even though they are below the surface. The descriptions of them are simply summarised on the following Table 6.

THE HARD ELEMENTS	
Strategy	Actions on a company plans in response to or anticipation of changes in its external environment
Structure	Basis for specialisation and co-ordination influenced primarily by strategy and organisation size and diversity
Systems	Formal and informal procedures that support the strategy and structure. (Systems are more powerful than they are given credit)
THE SOFT ELEMENTS	
Style/Culture	The culture of the organisation, consisting of two components: **Organisational Culture:** the dominant values and beliefs, and norms, which develop over time and become relatively enduring features of organisational life. **Management Style:** more a matter of what managers do than what they say; how do a company's managers spend their time? What are they focusing attention on? Symbolism – the creation and maintenance (or sometime deconstruction) of meaning is a fundamental responsibility of managers.
Staff	The people/human resource management – processes used to develop managers, socialisation processes, ways of shaping basic values of management cadre, ways of introducing young recruits to the company, ways of helping to manage the careers of employees
Skills	The distinctive competences – what the company does best, ways of expanding or shifting competences
Shared Values/Superordinate Goals	Guiding concepts, fundamental ideas around which a business is built – must be simple, usually stated at abstract level, have great meaning inside the organisation even though outsiders may not see or understand them.

Table 6 - Descriptions of the hard and soft elements of McKinsey's 7-S Model[104]

[104] Cf: Avner Barnea (2008), pp. 51-52

Effective organisations manage and put all these seven elements into action simultaneously. The McKinsey's 7-S Model is an important and helpful tool to implement change processes and to give them direction. The change management concept has been entirely explained up to now, and from now on we know how to handle and deal with any changes in an organisation, the next step will be the broad explanation of the challenges and difficulties to the introduction and implementation of an effective operational risk management into an organisation which will cause some changes to be managed successfully by the aid of change management practices which have been introduced so far.

The key challenges in implementing Risk Management including Operational Risk Management challenges and difficulties have been determined as follows by the collaborative Working Group that consisted of Australasian Institute of Risk Management, ISO Working group – Risk Management Terminology, Standards Australia / Standards New Zealand, Joint Technical Committee OB/7 – Risk Management.[105]

- *Board/CEO Support*
- *Responsibility/Accountability*
- *Risk Measurement*
- *Link to Corporate Strategy*
- *Link and impact of changes to good Corporate Governance*
- *Adding value*
- *Common risk language*
- *Management buy-in*
- *Link to control self assessment*
- *Risk reporting*
- *Technology*

4.2.1 Board/CEO Support[106]

- The lack of Board/CEO commitment or a limited supervision from them causes operational risk management system not to fulfil its functionality properly as it is expected and thereby the organisation cannot achieve or reach its pre-determined objectives and the chance of organisational success. Therefore,

[105] Kevin W. Knight (2003), p.16
[106] Cf: Kevin W. Knight, (2003), pp. 17 - 22

the full support from Board/CEO is a must and key success factor of gaining an effective risk management implementation.

- The Board has to realise and consider risk management and its necessary operations as a cost “reducer” or “avoider” rather than a cost addition. In addition to that point of view, if top management does not pay the same attention on risk management by their thoughts or behaviours as they value other management concepts within the organisation e.g. human resources project, or production management, the personnel will not respect that relatively new management discipline and take it into account in the way the management do.
- Hence, top management support is required on behalf of organisations in order to point out the tangible, understandable and feasible benefits of operational risk management for convincing the key stakeholder and thus receiving support of them for this management discipline.

4.2.2 Responsibility/Accountability

- One of the most important challenges concerning this issue is that risk manager’s responsibilities and authority are limited, and unclear.
- Another difficulty to implement operational risk management into an enterprise in terms of responsibility is that there is any existing risk orientation or awareness program for senior management, executive or personnel.
- It is needed to integrate assurance events with risk management and compliance.
- Concerning the first issue, role, borders, and the responsibilities of the entire Operational Risk Management team as well as Chief Operational Risk/Risk Officer should be clearly and precisely determined and described. The determination and description of the roles and responsibilities of the entire Operational Risk Management team will be comprehensively done in the following part of this chapter.
- An organisation should take the determination of responsibilities into account seriously while asking itself and answering the question of where risk management fits within its organisation. Because effectively and correctly determined responsibilities ensures the involvement of other functional skills within the process.

4.2.3 Risk Measurement

- It is necessary for organisation specific scales to forecast how often specified events may occur and the amount of their consequences.
- Risk measurement is the transition of measurement from qualitative views to quantitative estimations.
- The challenge or difficulty concerning risk measurement can be that the organisation does not have any standard processes, procedures, methods, or tools to measure and quantify all types of risks it faces. Thus there will be some incorrect approximations and the possible outcomes of these incorrect approximations, and impact of them on the success of organisational goals.

4.2.4 Link to Corporate Strategy

- Implementation program of Operational Risk Management should be linked to the corporate strategy of the organisation due to the requirement for tailored integration of it with business strategy.
- An adaptable Risk Management program which is successfully and precisely integrated with the corporate business strategy ensures that risk management team of organisation is taking the right risks confidently and managing the consequences of them rightly for success of the organisation.
- Changing to the culture of managing strategic as well as operational risks is managed by predicting, analysing, caring, preparing and preventing risks which are based on chance, unpredictability and opportunity. The achievement of changing the culture is understood and gained by effective and regular communication, consultation and monitoring during the whole process. The establishment of successfully changed risk management culture within the organisation leads to confidence, value and performance on behalf of organisation.
- In order to clearly understand and embed what we talked about the last issue above, it is necessary here to define what a risk management and risk culture are. The risk culture in an organisation is described in this manner;[107] *"This means that all our business behaviours relating to our individual performance encompass informed decisions to do or not to do things based on a reasonable analysis of foreseeable risks, opportunities and their associated impacts on the corporate objectives."*

[107] Kevin W. Knight (2003), p.19

4.2.5 Link and Impact of Changes to good Corporate Governance

- The ability of Operational Risk Management Standard which the organisation has to comply with should be proactive in order to allow directors to enable to fulfil their corporate governance responsibilities.
- The challenge about this issue can be that there is no corporate process in the organisation for identifying good practices of operational risk management or documenting them and further linking them with corporate governance.
- The above-mentioned difficulty so-called challenge can be prevented by the establishment an integrated management system which ensures progress in strategy implementation. This can be achieved by Figure 13 as follows.

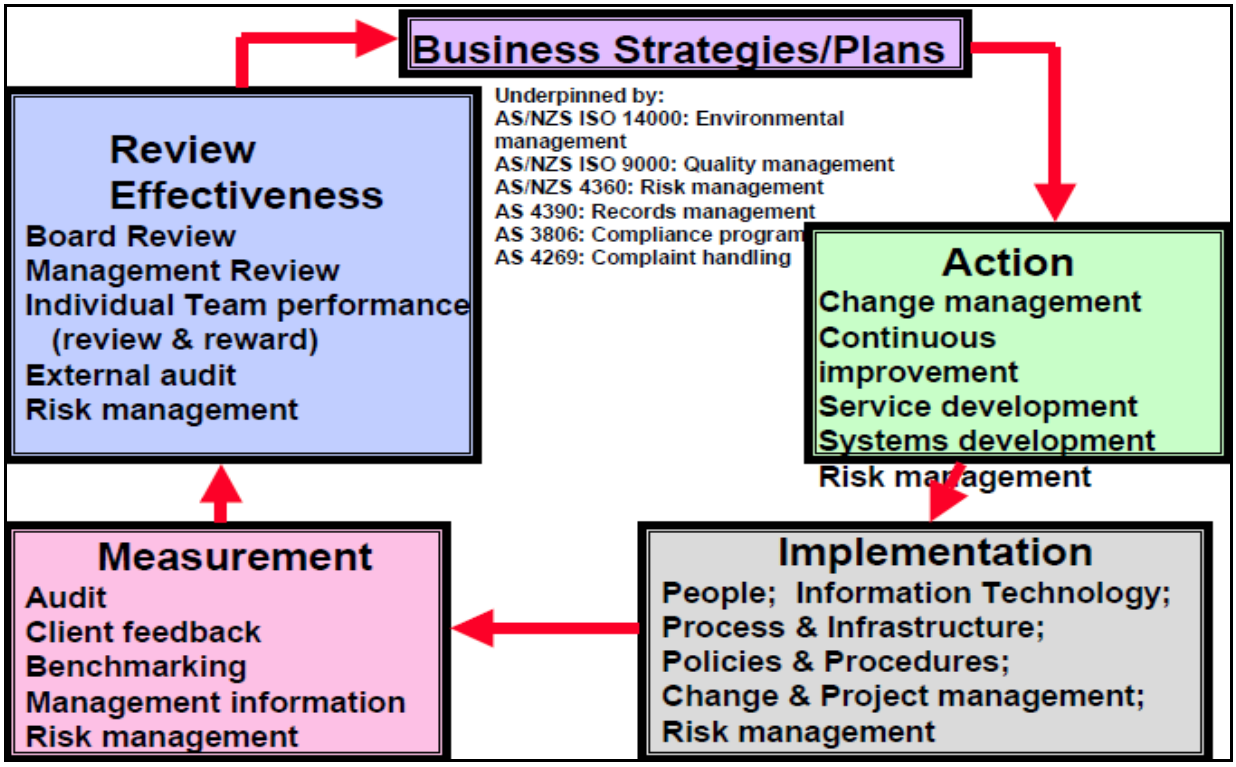


Figure 13 - An integrated management system in strategy implementation[108]

- It would be useful to define what the above-depicted integrated management system is. An integrated management system which is abbreviated as IMS is defined as follows;[109] *"An integrated management system (IMS) is a system which integrates all parts of business into a coherent system. It's a closed-loop management system. All elements are independent."*

[108] Kevin W. Knight (2003), p.31
[109] Dipl. - Ing. Dr. Techn. Werner Leitner, Dipl. Ing. Vladimir Valastiak (2009), p.4

4.2.6 Adding Value

- Adding value is the necessity to set up processes to connect strategic operational risk management with value creation and competitive advantage.

- The horizon and understanding of adding value should be broaden. In this sense, the thoughts and explanations of Bronwyn Friday will be utilised in order to enhance and enlighten the adding value approach;[110] Bronwyn Friday is the person who is the corporate risk manager at Citipower Pty. & Powercor Australia Ltd. and she was awarded as the Young Risk Professional of the year by Australian Risk Management Award 2005. In her article we utilise, she has searched and tried to figure out the answer of the question whether enterprise-wide risk management could add value or just protect the value of organisation. She has noticed that return on any business investment and its value generation over time had a clear understanding and was easy to quantify and measure in financial terms to stakeholders. In parallel to that, it was not obvious for many organisations how much risk they want to accept in order to add this value to their organisations due to risk measurement/quantification was not always an easy task to do. Sometimes the outcomes of a risk-related event could not be expressed financially, because these consequences could occur such as injuries, deaths, or loss of confidence. It is therefore a complex process to connect the individual risks with their related value, while also determining the real desire of an organisation which had to take these risks.

- So, according to Ms. Friday the answer of above-asked question is yes. The answer is yes and feasible for organisations which are completely aware of that Risk Management and its specified practices e.g. Operational Risk Management, Supply Chain Risk Management and so on are more than a management discipline or a methodology. Hence, the answer is yes for organisations which recognise Risk Management as a philosophy on how to make better decisions and to make every opportunity optimal to gain its greatest value while protecting the existing value of organisation at the same time.

[110] Cf: Bronwyn Friday (2006), (Consulted on 12.11.2009)

- She underscored that risk managers should keep in mind that the real implementation of an Enterprise Risk Management program created value in itself. She recommended further according to her experiences in a private electricity utility that the greatest value coming from the development of a corporate risk management program into an ERM system, is the development of physical, financial, and cultural resilience in all businesses of us, while still concentrating on gaining all business objectives of us. In addition to that, she defined resilience as follows; resilience can be the ability of an organisation which is gained by a successfully and properly implemented risk management system and lets organisations to return very quickly to their previous level of success, after they are affected by an incident.

- Meanwhile, in order to sum up the adding value part, we should look at the following figures (Figure 14 and Figure 15) carefully which clearly symbolise the trade-off between level of risk (risk value) and cost of reducing risk as well as the correlation between level of risk and risk magnitude.

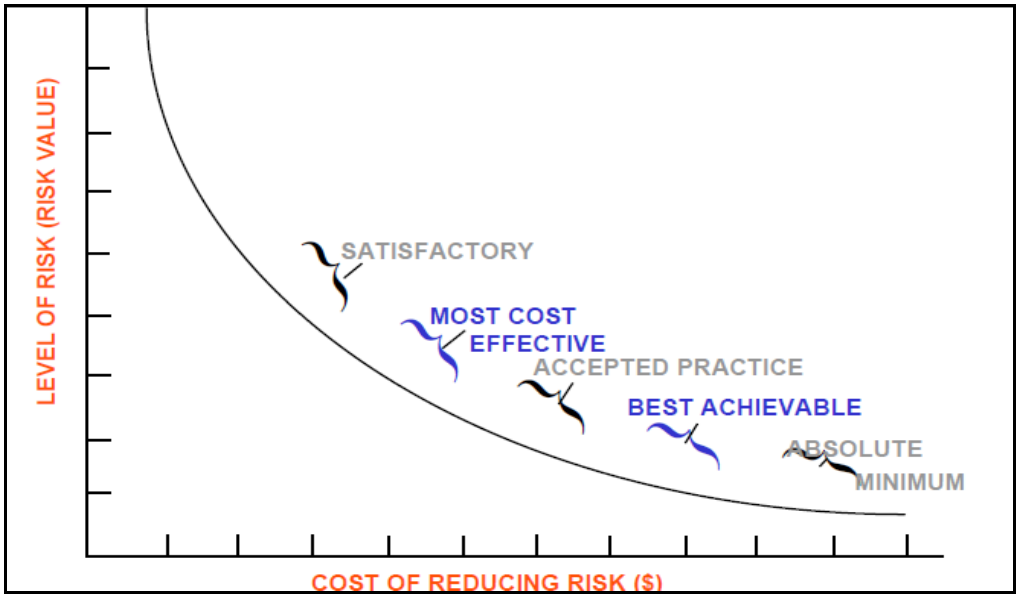


Figure 14 - The trade-off between level of risk and cost of reducing risk (B.F. Hough 1985)[111]

- Before the conclusion of adding value part, we should once again refer the opinions of Ms. Friday concerning risk appetite which is explained by the relation between the levels of risk an organisation faces and risk tolerance level with their quantification methods e.g. qualitative risk matrix, or table. She mentioned in her article that one of the first steps in developing an Enterprise-

[111] Kevin W. Knight (2003), p.36

wide Risk Management program is to guide organisations to achieve a practicable understanding of what risk levels are acceptable and develop a risk appetite matrix or tolerance tables to fit their needs. In this sense, organisation should keep in mind that it is important for them to provide tailored templates that are gained by Risk Management Standards, e.g. ISO 31000:2009 and etc. as well as fit their individual requirements. She further pointed out that if establishment of a qualitative risk matrix is too complex, then the development of an "As Low As Reasonably Practical (ALARP)" can a minefield. Because risk managers have also to convince top management and board to sign off on the level of risk that they suppose, while they have to sell the concept of how an ALARP table is used. The ALARP level that Ms. Friday underscored can be readily seen on below depicted Figure 15.

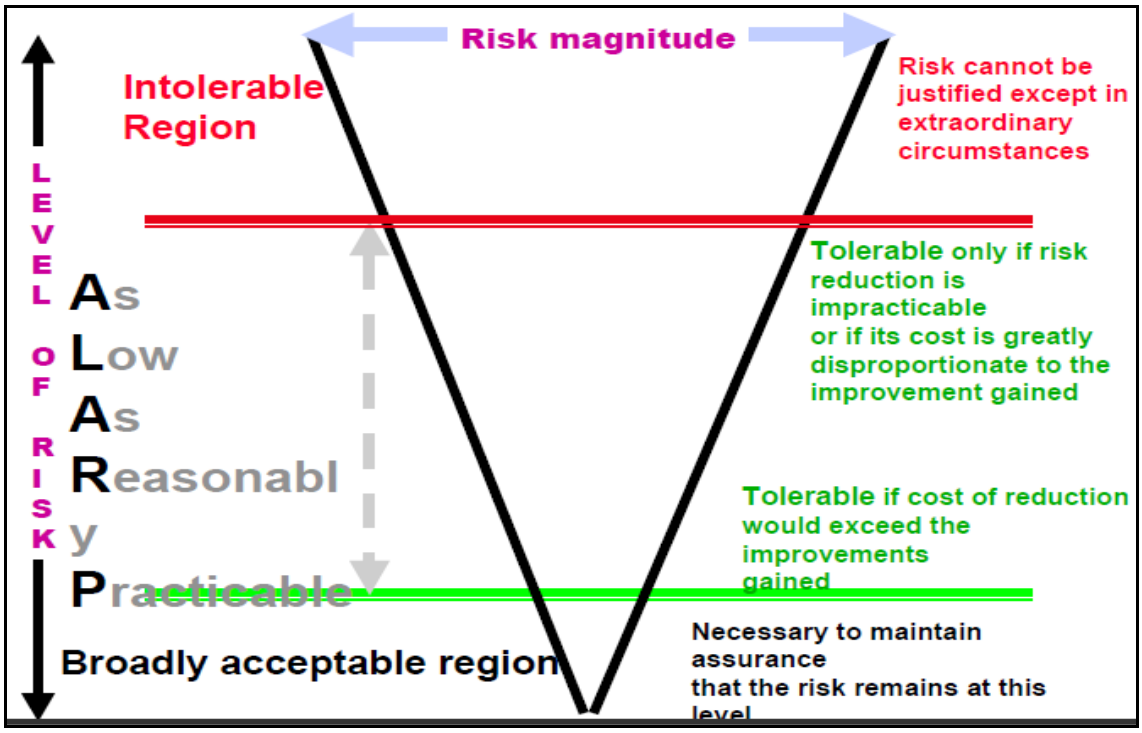


Figure 15 - Level of Risk – Risk Magnitudes[112]

4.2.7 Common Risk Language

- Establishing a common risk language within the organisation is closely associated with the 8th implementation step of an effective operational risk management model which we have comprehensively explained before and is so-called "break down the silos". In addition, the first and most important reason for having an organisation-wide risk language is to broaden the risk

[112] Kevin W. Knight (2003), p.37

culture of organisation that we also talked before about. Regarding breaking down the silos, most organisations have several layers e.g. senior managers, line managers, and personnel as well as they also have silos which we have mentioned before e.g. quality management, operations, and many others. Having common risk language is therefore needed to cut through the layers and break down the silos. In other words, without a common language risk management team can encounter many challenges concerning effective communication, understanding each other due to different point of views, understandings, translations and interpretations of a risk, when a risk is at stake.

- Successfully implemented common risk language ensures that everybody throughout the organisation has the common way of speaking and understanding about risk. Organisations have many languages of operational risks, unless the silos are broken down. Moreover, many languages of operational risks in an organisation will cause various and several definitions of ORM which will be made by different silos who are not communicated and aware of each other, despite they are working in the same organisation. However, different ORM definitions and concepts lead to confusion among the personnel and allow organisation not to have a common corporate risk culture as well.

- The observations of Ernst & Young regarding above-mentioned confusions as well as the challenges of having a common risk management language are remarkable. According to Ernst & Young consultants;[113] an organisation should ensure that everyone speaks the same risk language throughout the organisation which leads to eliminate the barriers to timely and efficient risk management struggles, and allows the organisation to define company-wide shared definitions, and priorities, as well as communication channels clearly and properly. It furthermore enables a common culture of risk awareness and accountability and clear procedures for measuring, monitoring, communicating, and dealing with risks. As a result, organisation that can achieve all we said above would be better able to create and protect value and gain a competitive advantage.

[113] Cf: Ernst & Young (2009), pp. 1 - 3

- In addition to the observations of Ernst & Young, it would be helpful to mention about some well-known common risk management dialects which also have been introduced by Ernst & Young. Those languages can be seen on Table 7.

Name	What it is
Hazard analysis and critical control points (HACCP)	It deals with physical, chemical, and biological threats to food and drugs safety.
SOX 404 Top down risk assessment (TDRA)	It is a financial reporting risk management tool to comply with section of the Sarbanes-Oxley Act of 2002.
Failure modes and effects analysis (FMEA)	It is a procedure for analysis and classification of the possible effects of failures on a system, very popular in manufacturing. It is now also used in the service industry.
Benchmark assessment tool (BEATO)	It is both a tool and methodology originally designed to check compliance in security assessments.
Probabilistic risk assessment (PRA)	It is a methodology for comprehensive assessment of risks associated with complex engineered constructions such as airplanes or nuclear power plants.

Table 7 - Some well-known risk management dialects

- As a conclusion, following classified four steps for developing a common risk management language in an organisation are crucial for organisations and must be paid more attention by organisations which would like solve and effectively manage the challenges they face regarding having a common risk management language. Only the organisations which can gather all below announced steps will be successful on the way of achieving a common risk language. Those steps are as follows:[114]

    1. *Develop a language for all*
    2. *Explain concepts simply and clearly*
    3. *Use real world examples*
    4. *Create a glossary*

[114] Donald Espersen (2007), pp. 1 - 2

4.2.8 Management Buy-in

- Management buy-in is defined as follows:[115] *"A corporate action in which an outside manager or management team purchases an ownership stake in the first company and replaces the existing management team. This type of action can occur due to a company appearing undervalued or having a poor management team."* In addition to definition, a manager who has significant and impressive managerial experience at directory level usually leads to the team.

- The comment of Midwest Audit Committee Network about Management buy-in is impressive and remarkable. The committee consists of leading Midwest (USA) companies like AEGON USA, Ernst & Young and so on. According to the committee;[116] *"You can have all the systems and procedures in the world, but without senior management buy-in, it is worthless."*

- Moreover, management buy-in is required to reduce the resistance to change; the operational buy-in will enable acceptance of responsibilities and the high and proactive level of top management's participation. If an organisation has a top management which is resistant to strategic communications that is considered as one of the key success factors, the very first step that should be taken can be to start working with top management to change their ideas and mentalities regarding the importance of strategic communication. Because an effective and successful implementation of the enterprise-wide Operational Risk Management can only be gained, if top management of the organisation believes in the importance of strategic communication as well as the value of implementation plan which is determined.

- The managing buy-in risk management checklist which clarifies the source of risks as well as risk reduction ideas can be seen on Table 8 below:

[115] Investopedia.com (Consulted on 17.11.2009)
[116] North Carolina (NC) State University (2008), (Consulted on 17.11.2009)

Source of risks	***Ideas for risk reduction***
Political Risk	***Assess organisational readiness for change*** • *Is Senior Management committed to the change effort to ensure that it gets appropriate priority and support?* • *Do the management and staff perceive that this change will improve the organisation and/or the environment in which people work?* • *Is there a sponsor or champion with adequate clout who strongly supports the project, to the extent that she/he is willing to fight to have the project succeed?* • *Are people, computer capacity, money and other resources available to implement the change effectively or are there other competing demands for resources that will receive higher priority?* • *Do the staff members have the necessary skills to work in the changed environment?*
	Set up a network to gather intelligence on what the key people are talking about – who speaks to whom, when and why, and any issues that may be developing.
	Use change influences analysis and resistance management techniques to analyse and address driving and opposing forces.
	Prepare specific commitment strategies and plans to obtain political support
	Establish overwhelming commitment to success at the executive level so that thoughts of failure are not permitted.
	Ensure key opinion leaders are directly involved in project team
	Lobby for votes ahead of time to ensure that you know the outcome of key meetings before you go in.
Schedule	*Use rigorous up-front planning and time-reduction analysis.*
	Plan for incremental implementation or phasing in of the change.
	Keep to the agreed-upon schedule.
	Add schedule management to the formal risk management plan to ensure visibility.

Table 8 continues on following page.

Table 8 continues as follows.

	Address schedule variances openly as they arise.
	Minimize any new changes or conditions which may impact the change effort (e.g. changes to staff, policies, and procedures).
Resistance	*Clearly define the target population's participation in the change effort.*
	Develop a plan for ensuring target population commitment
	Ensure personal and change effort objectives have been reconciled.
	Hold frequent meetings to facilitate communication, develop team spirit, and allow issues to be discussed.
	Provide incentive to motivate performance.
	Ensure that the target population is aware of change through regular status report.
	Meet with individuals as needed to address serious concerns and resistant behaviours.
	Arrange for target population representation on core change implementation teams.
Training	*Develop a training program and accompanying training plan.*
	Install a training infrastructure (e.g. help-desk, toll-free telephones support).
Quality of Change Effort	*Create a core team to define standards in advance.*
	Ensure that standards are formally documented, easily accessible, and easily understandable.
	Provide early feedback on adherence to standards.
New/Unknown Technology	*Provide for training*
	Provide comprehensive orientation
	Bring in temporary external resources to help get people up and running
Lack of Sponsorship	*Clearly define specific areas of sponsor's responsibility*
	Obtain executive commitment to provide adequate backing and resources.

Table 8 - The managing buy-in risk management checklist[117]

[117] Craig Borysowich (2007), (Consulted on 17.11.2009)

- The above-announced sponsor or champion, in this sense so-called Operational Risk Management Champion is in charge of facilitating risk management programme and reporting to the Board Risk Management Committee.

4.2.9 Link to Control Self Assessment

- Operational risk management implementation practices should be linked to control self assessment in order to integrate and compare top down strategic risk management process to bottom up control self assessments. In order to provide linkage between risk management practices and control self assessment, organisations should take into account what existing controls are put in practice and whether they are efficiently implemented and executed or not? Then the question arises whether these controls help or hinder the organisational ability to manage risks.

- "Control self assessment has been suggested and developed by auditors as a new concept to auditing in the late of 1980's. One of the reasons of its necessity was the probability of huge losses due to inadequately integrated operations; productivity decreasing from low staff morale, as well as misunderstandings because of business culture differences was extremely high, if above-mentioned changes or others were not appropriately executed. Thus, many modern corporations' departments were suffered from these changes, including auditing. Therefore many auditors have considered expanding the control evaluation in addition to the scope of traditional audits which could not significantly address several new business risks created by unlimited changes.

- Control Self Assessment (CSA) has therefore been developed to enhance and extend the conventional audit function. CSA is a dynamic, interactive process in which self-monitoring teams in facilitated workshops identify three things:

    1. The ongoing challenges of meeting business objectives
    2. The adequacy of controls to deal with these challenges
    3. The mitigation measures needed to address identified risks

- Moreover, the structure of internal control has been improved from a traditional based top-down financial model to a more flexible model which was an enterprise-wide one and able to link and integrate business risk management with continuous improvement and change. As a result, CSA aims to integrate (operational) risk management practices and culture across the organisation and business units/departments achieve their objectives." [118]

- By the way, an organisation can face some challenges and difficulties concerning Internal Audit – Risk / Control Self Assessment due to some reasons. Those reasons are determined by PricewaterhouseCoopers Consulting firm as follows:[119]

    1. *Management does not have awareness of risk management.*
    2. *Management does not understand the risks they are facing in their business.*
    3. *The company has not documented, prioritised nor quantified the risks of their business.*
    4. *Management makes no effort to forecast or predict where problems could arise.*
    5. *Annual audit plan is not prepared based on the results of a risk assessment.*
    6. *…*

4.2.10 Risk Reporting

- It is necessary to design convenient reports to assist and help management as well as to make decisions in accordance with risk management principles.

- Moreover, organisations should ensure that they have got the convenient risk tools which help them in identifying and reporting risks. Besides they also make sure that data they obtain should be easily able to be utilised as management information. Because we have underscored before that management complains about having a lot of data, but having a few information to use. So, effective risk reporting is the key to provide useful information to management to use.

[118] Cf: Noreen Foh (2000), p. 1
[119] PriceWaterhouseCoopers Hong Kong (2002), (Consulted on 18.11.2009)

- In sum, effective risk reporting reduces cost of compliance, while simultaneously adding value to the organisation, as it has been stated within a recent investigation of PricewaterhouseCoopers. The study says:[120] *"- a recent study by PricewaterhouseCoopers ranked over-regulation as the greatest threat to the Australian Insurance industry – more efficient risk reporting could lower costs as well as adding value."*

4.2.11 Technology

- Technology plays an important role in implementation of an effective operational risk management. It is therefore required for consistent methods for warehousing and risk reporting management data that have been acquired along the organisation.

- There are some roles of technology in risk management have been determined. There are basically four major areas where technology plays a role in any risk management practices. Those roles are as follows:[121]

    1. *Data collection and storage*
    2. *Risk analysis and modelling*
    3. *Risk monitoring and control*
    4. *Risk information and communication*

- In accordance with the above-announced roles, we can clearly and readily say that technology plays a key role during the entire risk management implementation process.

- Before we conclude the technology part, it would be helpful to have a look at the observations of Deloitte & Touche LLP concerning the role of technology in the implementation of an effective risk management:[122] "*According to Deloitte's recent poll, finance industry managers believe that they need to improve several dimensions of risk management technology. Nearly half (46%) say that they have to improve modelling tools to analyse multiple risk scenarios. Others report that they need to improve either cross-asset modelling and reporting (22%) or extensibility to easily add complex products (21%), while 11% say that they need to improve effective limit management."*

[120] Stuart Fagg (2009), (Consulted on 21.11.2009)
[121] Mike Wilkinson (2009), p.2
[122] Deloitte Financial Services (2008), pp. 2 - 4

In addition to that, the above-mentioned percentages can be easily seen on below-illustrated Figure 16.

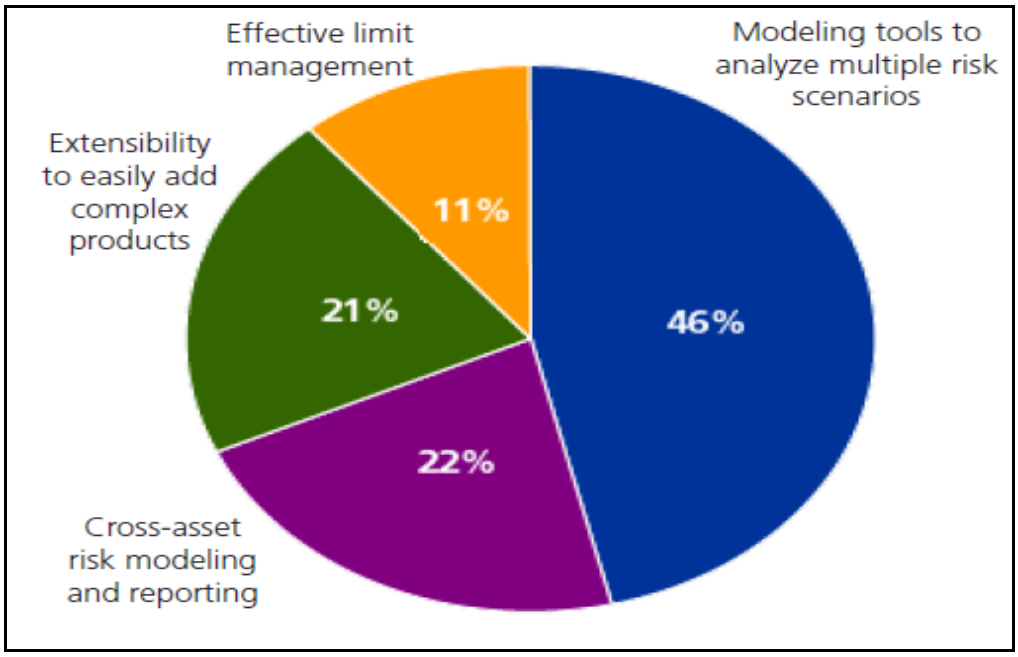


Figure 16 - Risk Management Technology improves the most in a firm

- Meanwhile, according to Deloitte & Touche LLP there are four types of IT solutions which investment managers have while determining IT solutions for their risk management systems. Those options are listed below with Figure 17 that represents their utilisation percentages by organisations.

    1. *Option # 1 – Buy*
    2. *Option # 2 – Build/Custom Development (Excel Spreadsheets)*
    3. *Option # 3 – Hybrid*
    4. *Option # 4 – Outsource*

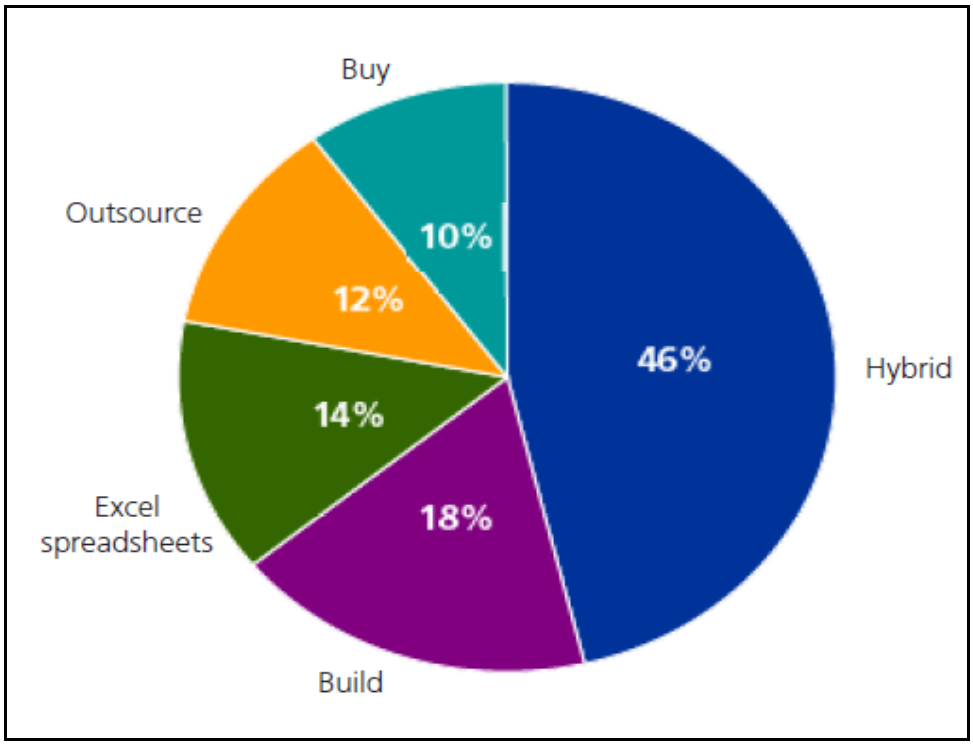


Figure 17 - The utilisation for risk management system selection by firms

As a conclusion of this chapter, we have comprehensively explained the major challenges to the implementation of an effective Operational Risk Management into an organisation so far. Once an organisation is clearly aware of what kind of challenges it faces, further determines them properly, while it aims to implement efficiently an ORM into its day-to-day operations and business life, it would be easier to handle or reduce those challenges or difficulties as well as their impacts on a tolerable level that affect the success of the implementation. After the challenges have been understood correctly, it is time to talk about the roles, and responsibilities of risk-related people so-called risk management team who are in charge of putting the implementation as well as all operational risk management practices into action, simultaneously performing and managing those operations within the organisation. So, the roles, and responsibilities of operational risk management team will be broadly explained and worked out in details in the following chapter.

4.3 Roles, and Responsibilities of Risk Management Team

The roles and responsibilities of Risk Management Team should be defined and determined properly in order not to face any challenges as well as difficulties, while an effective Operational Risk Management System is implemented throughout the organisation. As we have underscored within the previous chapter, the division of jobs within the team, determination of responsibilities, roles as well as the

responsibility borders of Risk Management Team are one of the important challenges of the implementation of the Operational Risk Management.

It would be important to talk about the position, role and responsibilities of the head of Risk Management Team who is also called Chief Risk Officer (CRO). The popularity, functionality and importance of CRO in an organisation have been arisen in recent years, even though it has been created as a new title in business world by James Lam in 1993. According to James Lam;[123] the story has begun in August 1993, while he was working as a consultant for Financial Guaranty Insurance Group at GE Capital. His job was to manage all aspects of risk and he had the direct responsibility for all functions outside of sales and trading, which consisted of risk management, back-office operations, and business and financial planning. Rick Price who was in charge of James Lam within the company has requested him to come up with a new title for what he was dealing within the company which was a new business.

Before James Lam came up with the idea of CRO, GE and other companies have assigned "Chief Information Officers" or CIOs in order to elevate the role of technology in business. Furthermore the CIO was commonly in charge of developing and implementing an integrated technology strategy which includes mainframes, PCs, networks, and internet. James Lam has put the CIO trend and his new responsibilities for market, credit and operational risks together and gathering all those has given him the idea for the role and title of "Chief Risk Officer" or CRO. According to Lam, the CRO would be responsible for developing and implementing an enterprise-wide risk management strategy which includes all aspects of risk.

In addition to that;[124] *"A cross-industry survey of 137 global firms by the Economist Intelligence Unit (EIU) found that:*

- *45% have already appointed a CRO or equivalent*
- *24% planned to appoint a CRO in the next two years"*

[123] Cf: James Lam (2000), p. 4
[124] James Lam (2008), p. 7

The recently-done survey which is underscored above remarkably points out the importance of CRO which is paid by enterprises around the world. Moreover, CRO was a commonly-used managerial position for financial corporations, when it has been invented in early 1990s. On the other hand, after some incidents and huge losses have happened due to operational, strategic, market risks and failures within the non-financial corporations, the importance of CRO management position has been also arisen for all kind corporations except banks and financial institutions. Once again, according to James Lam, CRO is generally and directly responsible for:[125]

- *Providing the overall leadership, vision, and direction for enterprise risk management;*
- *Establishing an integrated risk management framework for all aspects of risks across the organisation;*
- *Developing risk management policies, including the quantification of management's risk appetite through specific risk limits;*
- *Implementing a set of risk metrics and reports, including loses and incidents, key risk exposures, and early warning indicators;*
- *Allocating economic capital to business activities based on risk, and optimizing the company's risk portfolio through business activities and risk transfer strategies;*
- *Improving the company's risk management readiness through communication and training programs, risk-based performance measurement and incentives, and other change management programs;*
- *Developing the analytical, systems and data management capabilities to support the risk management program.*

By the way, the position of a Chief Risk Officer is a C-level management position which stands for Top-level Executive like Chief Executive Officer (CEO), Chief Operating Officer (COO) and etc. According to Peter den Dekker who is the president

[125] James Lam (2000), p. 4

of FERMA (The Association of European Risk Managers);[126] *"The CRO is member of the board and part of the corporate decision-making body. He or she will be taking part in decisions about mergers and acquisitions, contracts, investments, and etc."*

A Risk Management team consists of Chief Risk Officer as the head of the team, but in some organisations which do not appoint a CRO, the CEO can replace and work as CRO at the same time. Besides CRO, other team members and risk-affected people in an organisation are as follows; team is lead by a Risk Improvement Manager (for public sector) or a Risk Manager (for private sector), other senior managers, a risk specialist, internal audit committee, and Line Managers so-called managers across the organisation as well as all staff. There can be found hundreds of different positional roles and responsibilities definitions of a risk management team. The exact determination of roles and positions of a risk management team can vary according to the size of organisation as well as what type of business organisations do. According to one approach of a risk management team can be seen on Table 9 below.

Role	***Responsibilities***
Accounting Officer (Chief Executive Officer)	• *Acts as the figurehead for the management of risk within the organisation*
Risk Improvement Manager (public sector) or Risk Manager (private sector)	• *Ensures the Operational Risk Management Framework is implemented* • *Carries out ongoing management of risk maturity assessments* • *Develops plans to improve management of risk* • *Develops management of risk guidance and training* • *Identifies lessons learned and disseminates learning* • *Undertakes risk management training and holds seminars to embed risk management* • *Develops a programme for the embedding of management of risk.*

Table 9 continues on following page.

[126] Lloyds.com (2009), (Consulted on 03.12.2009)

Table 9 continues as follows.

Programme, project and operational unit boards, senior responsible owners	• *Understand the Operational Risk Management Framework and their accountabilities* • *Implement the Operational Risk Management framework within their areas of responsibility* • *Escalate programme, project and operational risks according to the strategic perspectives defined in the Operational Risk Management framework* • *Promote management of risk principles* • *Manage the risk associated with programmes, projects and operational areas.*
Risk Specialists	• *Prepare strategic Risk Management Plans including education, training, awareness and cultural embedding plans* • *Undertake qualitative and quantitative analysis with management* • *Prepare risk management reports.*
Internal Audit Department	• *Makes formal assessments of management of risk implementation in areas of concern* • *Assesses the controls in place to manage, mitigate or reduce risks.*
Managers across the organisation	• *Review and manage risk controls within their area of responsibility within the organisation* • *Promote management of risk and its principles to their staff.*
All Staff	• *Help identify and report or escalate risks to management.*

Table 9 - Roles and Responsibilities[127]

On the other hand, another risk management team form can be sketched on Figure 18. On the figure, the roles, duties and interaction among the team can be seen.

[127] Office of Government Commerce (OGC), "Management of Risk: Guidance for Practitioners", (2007) p.62

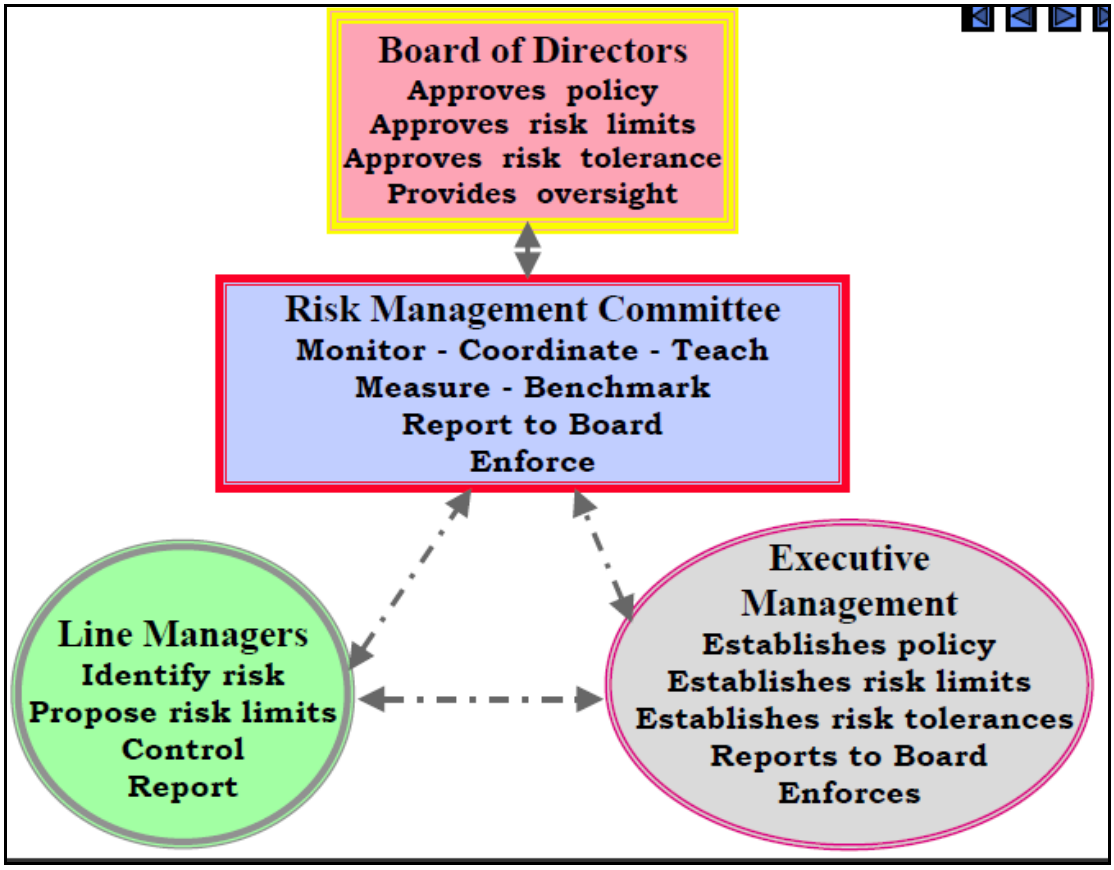


Figure 18 - The Risk Management Team Formation[128]

4.4 Summary

Implementation chapter has been explained comprehensively so far. The implementation steps, challenges and difficulties of the implementation of operational risk management in an organisation, and lastly the roles and responsibilities of risk management team which realises the implementation concept and put it into action have been told step by step.

Once the entire implementation method and its supplementary components are understood clearly, it is time to realise and embed it by the aid of a case study which will be broadly explained in the following chapter and interpreted once again step by step according to the Risk Management Process Diagram that has been drawn in Chapter 2.

[128] Kevin W. Knight (2003), p. 41

5. CASE STUDY

This is the last but not least chapter in which a case study from a chosen industry will be interpreted and explained broadly in accordance with the previously illustrated Risk Management Process Flow Chart. This chapter allows the readers and industrial practitioners to take the advantage of proper understanding and embedding the entire concept of Operational Risk Management.

Nevertheless, the chosen sector will be the automotive industry, and the type of Operational Risk Management which will be investigated will be Supply Chain Risk Management (SCRM). So the concept of the case study will be “The Supply Chain Risk Management in Automotive Industry”.

5.1 The Supply Chain Management in Automotive Industry

The reason of why we have chosen supply chain risk management is that we have previously mentioned about the increasing importance of risk management in Supply Chain Management by the remarkable Ericsson’s supply chain disruption story which has not handled professionally and therefore caused a business discontinuity in the name of Ericsson. Now we would like broaden the horizon of Supply Chain Risk Management by putting it in practice within automotive industry which is more complicated than mobile phone manufacturing sector in terms of Supply Chain due to there may be hundreds of different suppliers an automaker or even a supplier can have. That means the SCRM plays a crucial role for automotive industry and it is a must have Operational Risk Management approach for organisations which play a direct or an indirect role (as an automaker, the supplier of this automaker or the sub-supplier of those enterprises) within the industry.

On the other hand, the below-depicted figure clearly points out the increasing importance of SCRM from the perspectives of manufacturing companies as well as logistics service providers. The Figure 19 can be seen as follows:

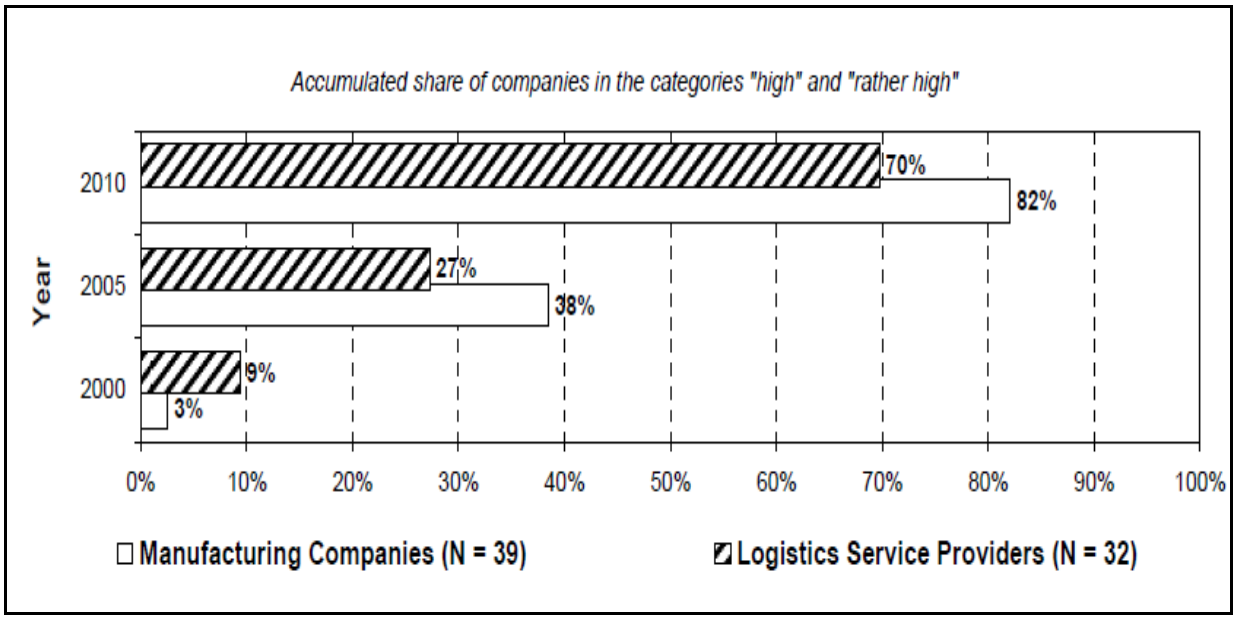
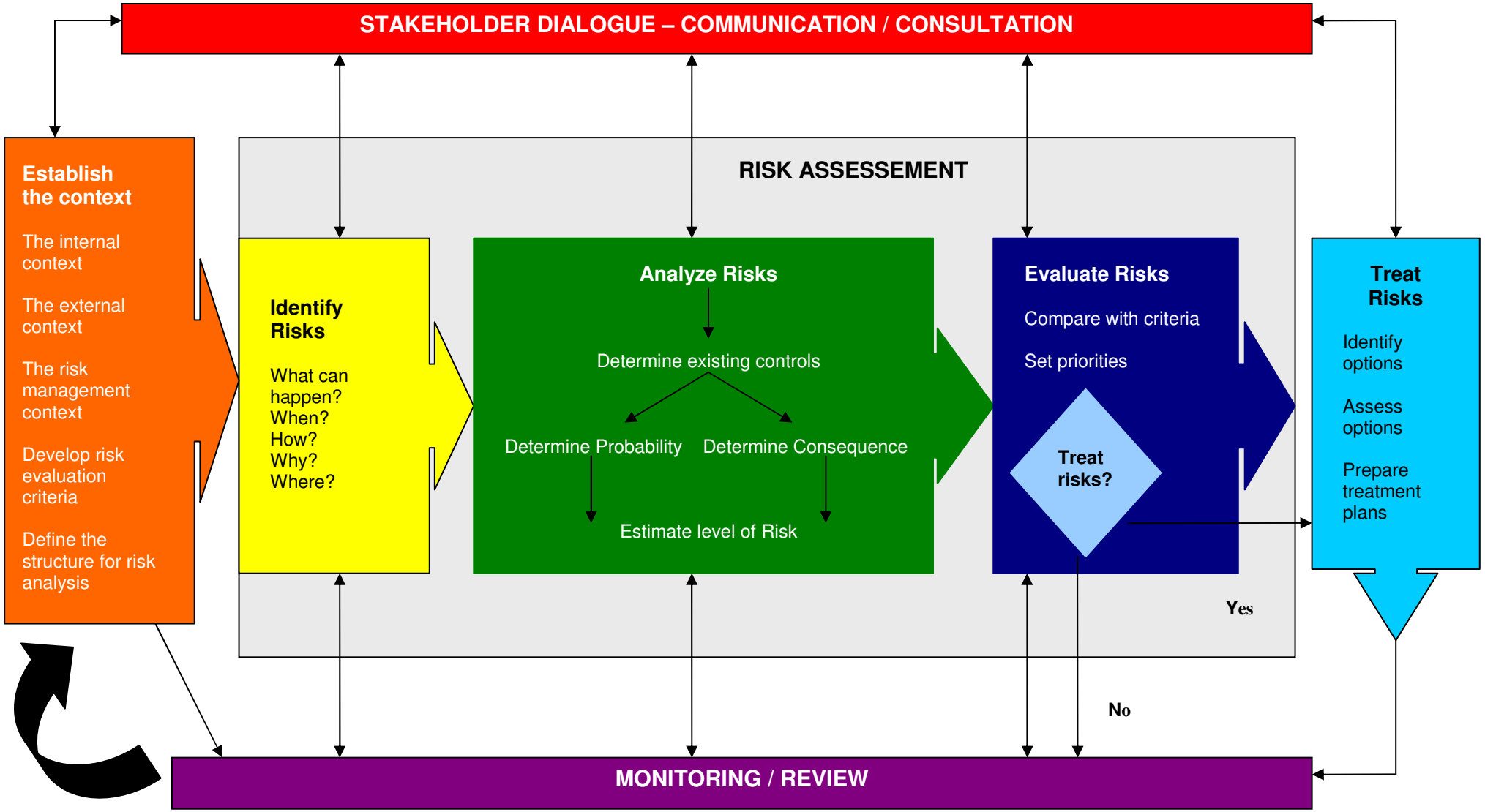


Figure 19 - Importance of Supply Chain Risk Management[129]

As it was stated before that the case study would be based on pre-determined Risk Management Process, it would be helpful to illustrate this Process once again in order to remind previously and broadly explained 7 steps of it. The steps of the Process can be seen on Figure 20 below.

[129] Wolfgang Kersten, Philipp Honrath & Maireke Böger (2007), p. 11

Figure 20 – Risk Management Process



The summarised details of the case study can be seen on Table 10 as follows:

Company Details	Necessary Information
Name	Anatolian Engineered Filters Ltd.
Headquarter	Istanbul/Turkey
Field	Liquid Management Systems for Vehicle and Engine Manufacturers
Number of Employee	500
Functional Departments	Operations/Production Management, Supply Chain Management, Product Research and Development, Sales and Marketing, Engineering and Maintenance, Finance & Controlling, Human Resources, and IT
Major Customers	Ford, Fiat, Magna
Key Supplier	Sao Paolo Filtration Systems Sao Paolo/Brazil
Supply Chain Risk Management Team (SCRMT)	• Chief Risk Officer (the head of SCM Department) • SCRM Consultant • Risk Officer from SCM • Risk Officer from Finance & Controlling • Risk Officer from IT • Risk Officer from Sales and Marketing • Risk Officer from Operations/Production
Hired SCRM Consultant	Boran ATES
Project	Implementation of Supply Chain Risk Management within the organisation

Table 10 - Summarised Case Study Details

The Anatolian Engineered Filters Ltd. is a Turkish company which manufactures Liquid Management Systems for Vehicle and Engine manufacturers like Ford Otosan, Fiat Tofas and Magna International etc. that are the major clients of the related organisation. The company is a middle-sized manufacturing company that has 500 employees who are working within the above-mentioned functional

departments as well as shop-floor. The key supplier of the company is Sao Paolo Filtration Systems which is based on Sao Paolo/Brazil and supplies main raw materials to Anatolian Engineered Filters Ltd. for Liquid Management Systems production. Product portfolio of Anatolian Engineered Filters Ltd. which stands for Liquid Management Systems for engines and vehicles consist of oil filter modules, fuel filter modules, carbon canister, heating and cooling modules, air dryers and oil and coolant pumps.

The increased competition, as well as increased expectations of customers, and globalisation of suppliers of automotive manufacturers made the Board of Anatolian Engineered Filters Ltd. to check out and review the important and key risks they face. At the end of Board meeting sessions with other executive managers, the Board found out that the source of major and key risks of organisation was Supply Chain Management (SCM), thus they decided to look deeper through the Supply Chain Risk Management (SCRM) and risks which will be occurred due to Supply Chain disruptions. The Board would like focus on Supply Chain related risks due to the major supplier of company is in Brazil where is relatively far from Turkey. In addition to that, there may be lots of risks can be happened from such a supplier which will cause huge losses in terms of money, company's reputation, bankruptcy and so on. Therefore, the Board has decided to implement a SCRM throughout the entire organisation in order to minimise supply chain related risks and their impacts, enhance and maximize the opportunities and chances to reach the pre-determined organisational goals and success.

In sum, the intention of the Board is to implement a SCRM approach to able to identify, analyse, and monitor the threats and risks on organisational success. In order to obtain this SCRM, the Board decided to develop and implement its own SCRM program which has not been existed before and thereof will be a completely new implementation project for the enterprise. The Board and executive managers had a meeting after the decision of Implementation of SCRM program has been made, the very first decision that has been taken in the meeting was to hire an external risk consultant as an advisor who would create a company profile. Because, it is a strategic decision to hire such a consultant for organisations which are aimed to take the advantage of different and experienced point of views that comes from outside of company. Hence, this external point of view helps to visualise the possible changes to be done in a good and successful manner.

After the decision of hiring an external risk consultant, the company hired Boran ATES who freelances as a Supply Chain Risk Consultant, has supervised and worked on several SCRM as well as other Operational Risk Management projects for local and multinational organisations. The duty of consultant is basically doing interviews to managers and personnel from different departments of the organisation to obtain an enterprise-wide point of view concerning organisational risk exposure in terms of SCM, and get and idea about the weak points of the future implemented SCRM program. At this point, Mr. Ates has proposed the Board to tailor and implement his own Risk Management Process that has been developed by him and experimented successfully on several local and international projects before. Besides, Mr. Ates's Risk Management Process consists of 7 steps which can be readily seen on above-drawn Figure 20. It would be useful to remind those seven steps once again, before they are put in practice. Those steps are as follows:

- Step 1. Stakeholder Dialogue – Communication/Consultation
- Step 2. Establish the context
- Step 3. Identify the risks
- Step 4. Analyse the risks
- Step 5. Evaluate the risks
- Step 6. Treat the risks
- Step 7. Monitoring and review

5.2 Step 1: Stakeholder Dialogue – Communication/Consultation

This step has been considered and called as one of the most important steps of the entire Supply Chain Risk Management Process (SCRMP) by Mr. Ates at the first SCRM Implementation Meeting. Moreover, it has been decided at the first SCRM Implementation Meeting that the meeting will be arranged weekly with the participation of Supply Chain Risk Management Team (SCRMT) including the external consultant, and monthly with the participation of the Board.

Furthermore, during the first meeting the importance of internal and external Stakeholders' Dialogue throughout SCM, Communication among the supply chain risk related and affected people during SCRM Implementation have been presented to the Board and further strongly underscored. The Board and other senior executives have asked Mr. Ates to cooperate with SCRMT and work closely together on the determination of SCM Stakeholders and possible stakeholder related risks. In addition to that, SCRMT worked on the determination of Stakeholders of SCM as well

as stakeholder related risks until the other meeting which has been executed by the Board and other senior managers. The results of the collaborative work from SCRMT can be seen on Figure 21 as follows:

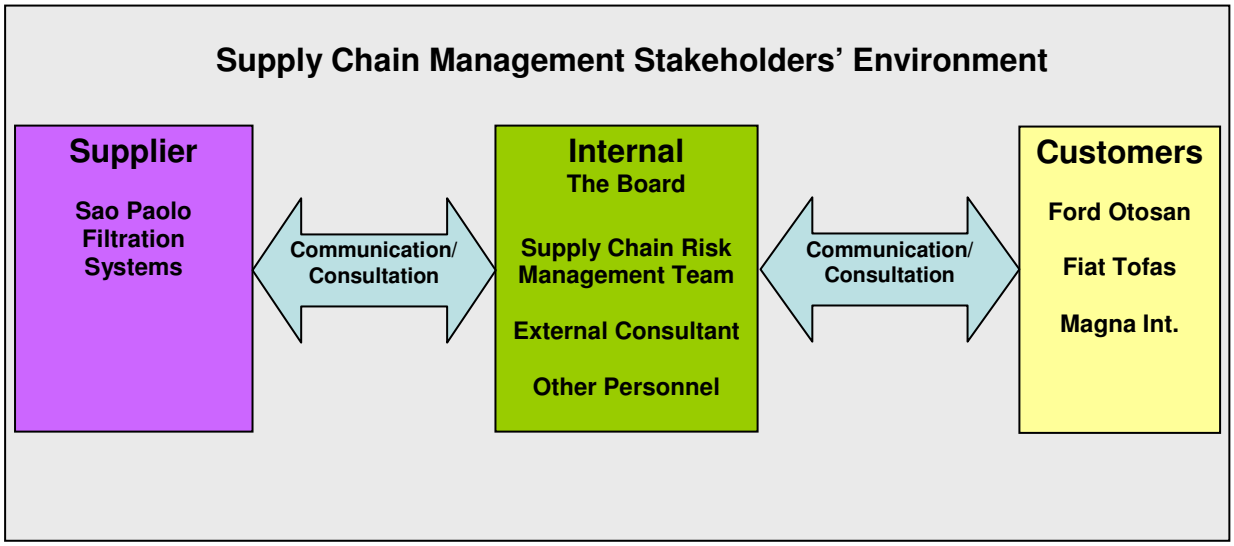


Figure 21 – Supply Chain Management Stakeholders

Once the determination of internal and external SCM Stakeholders of Anatolian Engineered Filters Ltd. is done by SCRMT, the next step is to determine stakeholder related risks that the organisation can encounter. This task has been realised after a comprehensive research about Managing Stakeholders within SCM has been done by SCRMT. On the following Table 11 the determined risks are classified.

Supplier	***Internal***	***Customers***
SC Disruption	*Environmental*	*Environmental*
Capacity / Quality	*Legal / Financial*	*Volume / Product mix*
Supplier Performance	*Technical / Operational*	*Brand / Reputation*
Supplier Environment	*Staff Turnover / OH&S*	*Data Sharing*
Financial Distress	*SC Disruption History*	*Product Liability*
Product/Process	*Capacity / Sourcing*	*Legal Liability*
Innovation	*Quality / Delivery*	*Market Mix Disasters*
Relationship	*Spend Leverage*	*Quality*
Regulatory	*Innovation*	
Disaster		

Table 11 – Risks – Managing Stakeholders[130]

[130] Anand Subramaniam (2009), p. 15

In the meantime, SCRMT arranged and led some internal workshops, meetings and training sessions in which they invited supply chain risks affected personnel in order to let them know and to be informed about how they can deal with and solve the supply chain related risks and specifically communicational risks within SCM and how they can effectively communicate each other throughout the SCRM process. During those meetings, trainings and workshops, SCRMT applied some techniques to inform personnel and let and encourage them to play an effective role in decision making process and easily share their ideas to improve SCRM process. Hence, these techniques have also been used to determine and find out solutions or recommendations for solving stakeholder related risks as well as communicational risks in SCRM process. Some determined communicational risks which have been found out by the aid of applying some techniques and the solutions/recommendations to handle and solve those risks can be seen on Table 12 below.

Communication Risks	**Applied Technique**	**Solution/Recommendation**
Cultural Differences	Internal Workshop Brainstorming	• Determine the cultural differences by brainstorming sessions • Invite a country expert to internal workshop to inform your personnel about the cultural differences

Table 12 continues on following page.

Table 12 continues as follows.

Language Barriers	Brainstorming Training	• Determine the language barriers by brainstorming sessions • Train your SCM personnel • Hire highly-qualified personnel who have multi-lingual abilities (Portuguese, German, English, Italian and etc.)
Misunderstanding	Cause – Effect Analysis Brainstorming	• Determine the root causes of misunderstanding by performing Cause-Effect Analysis • Apply above-mentioned recommendations to solve misunderstandings caused by above-mentioned risks • Find out and list previously happened misunderstandings and their impacts by brainstorming

Table 12 - Communicational Risks – Applied Techniques – Solutions/Recommendations

Once SCRMT has ensured that effective communication/consultation and stakeholder management have gained throughout the entire SCRM Implementation, the next step which will be implemented is establishment of the context. By the way the first step has been kept to be applied during the entire SCRM Implementation

due to it is a complementary step of the whole process as it can be seen on Figure 20 above.

5.3 Step 2: Establish the Context

Mr. Ates's Risk Management Process includes a five-step process to assist according with establishing the context within that risk will be identified. Those steps are named as follows:

1. The internal context
2. The external context
3. The risk management context
4. Develop risk evaluation criteria
5. Define the structure for risk analysis

The SCRMT worked further on the above-mentioned sub-steps in order to implement this step successfully.

1. Establish the internal context

The task of SCRMT was to identify the objectives and goals of the project so-called "The Implementation of Supply Chain Risk Management within the organisation". In order to do this, SCRMT organised an internal meeting, invited Senior Managers as well as the Board. They finally determined the objectives and goals of the project by reviewing pre-determined objectives and goals of the organisation as well as interviewing and consulting Senior Managers and the Board. The identified goals and objectives of the project are as follows:[131]

The Objectives of the Project

- Establishing mitigative and contingent strategies for how to deal with the identified risks and their potential impact on the supply chain
- Identifying and prioritising critical business elements
- Identifying and understanding the specific drivers that increase supplier risk
- Mapping the entire supply chain to show interdependencies
- Identifying potential failure points along the supply chain

[131] Cf: Ericsson (2004) p. 5, Hewlett-Packard (2006) p. 3, Supply Chain Council, Inc. (2009) p. 22, Industryweek.com (2008) p. 2

The Goals of the Project

- Embedding risk awareness into all core elements of the organisation, from C-level management through supervisors and department heads across the various supply chain functions
- Minimising risk exposure in the supply chain
- Better and strengthened SCRM coordination and relationship with customers, suppliers, and stakeholders
- Managing demand successfully, while reducing costs of the impacts of supply chain related risks and increasing revenue growth at the same time

After the objectives and goals has been identified and presented to Board as well as all supply chain affected personnel, SCRMT asked some questions to organisation in order to find out what existing staff groups they have and what capabilities they have in terms of people, systems, processes, equipment and other resources. SCRMT found out the organisational chart of their team as well as responsibilities of them. In addition to that, they represented a proposed framework of IT integrated Supply Chain Process Structure (SCPS) in order to explain what capabilities they have in terms of the entire SCM concept. The organisational chart of SCRMT, their roles and responsibilities can be seen on following Figure 22, Table 13.

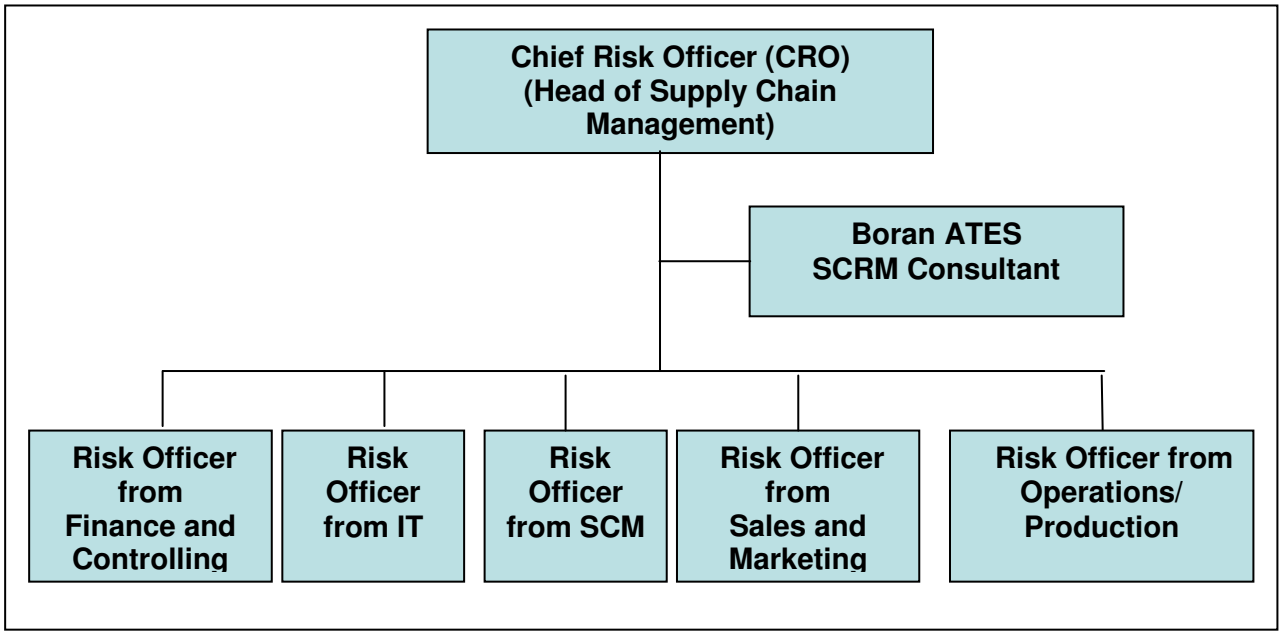


Figure 22 – Organisational Chart of SCRMT

Role	Responsibilities
Chief Risk Officer (CRO)	• Acts as the head for the SCRM within the organisation
SCRM Consultant	• Ensures the SCRM Framework is implemented • Carries out ongoing management of risk maturity assessments • Develops plans and programmes to improve and embed SCRM • Develops management of risk guidance and training • Identifies lessons learned and disseminates learning • Prepare and undertakes strategic SCRM Plans including education, seminars, training, awareness and cultural plans to embed SCRM • Undertake qualitative and quantitative analysis with management
Risk Officers from various departments (Finance & Controlling, SCM, IT, Sales & Marketing, Operations & Production)	• Understand the Supply Chain Risk Management Framework and their accountabilities • Implement the Supply Chain Risk Management framework within their areas of responsibility • Escalate programme, project and supply chain related risks according to the strategic perspectives defined in the Supply Chain Risk Management framework • Promote management of risk principles • Manage the supply chain risk associated with programmes, projects and operational areas. • Prepare SCRM Reports.
All Staff	• Help identify and report or escalate risks to management.

Table 13 – Roles and Responsibilities of SCRMT

Meanwhile, the proposed framework of IT integrated SCPS is shown on Figure 23 below:

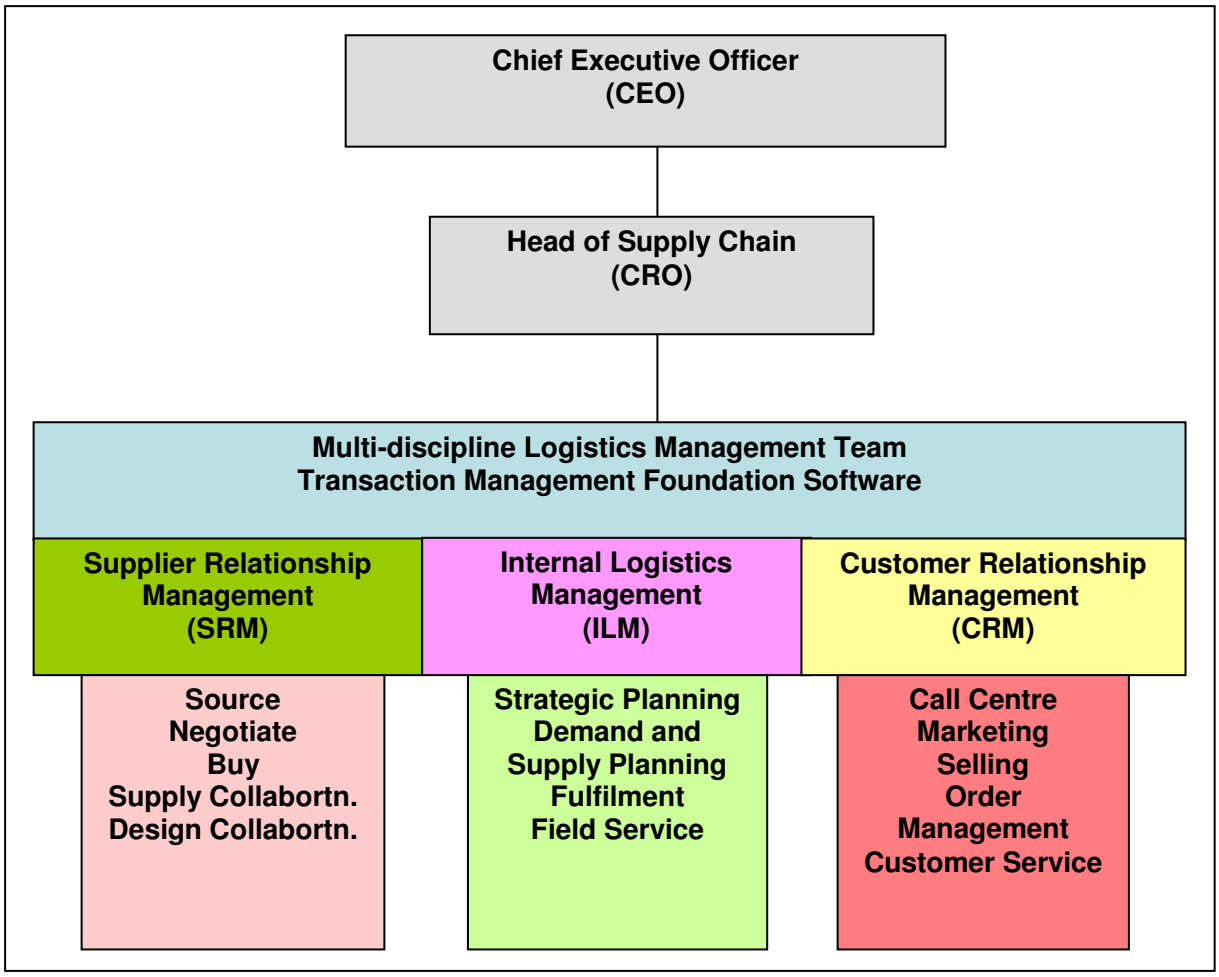


Figure 23 - Proposed Framework of IT integrated SCPS[132]

2. Establish the external context

In this step, the task of SCRMT was to review and control whether the external context in terms of legislative, regulatory, political and environmental compliances has been complied with or not. If not, the task is to determine what additional compliances should be complied with. SCRMT has checked previously complied standards and confirmed that all necessary compliances have been provided. Some certifications and standards that Anatolian Engineered Filters Ltd has had and complied with can be seen on Table 14 as follows:

[132] Cf: Vikram S. Tyagi (2007), p.14

Standards & Requirements	Responsible Dept.	Situation
ISO 9001:2008	Total Quality Management (TQM)	Certified
QS 9000 Quality System Assessment (QSA) Advanced Product Quality Planning and Control Plan (APQP) Production Part Approval Process (PPAP) Failure Mode and Effects Analysis (FMEA) Measurement System Analysis (MSA) Statistical Process Control (SPC)	TQM	Certified
ISO TS 16949:2009	TQM	Certified
OHS **(Occupational Health and Safety)**	TQM	Certified
SAP SCM – ERP – CRM Solutions	SCM and SCRMT	Registered

Table 14 - Standards & Requirements, Responsible Department, Conformational Situation

3. Establish the risk management context

In this step, the risk management context has been implemented by SCRMT, as it is shown on Table 15 below:

Determination	Explanations
Primary Objective of Project	Establishing mitigative and contingent strategies for how to deal with the identified risks and their potential impact on the supply chain
Primary Goal of Project	Embedding risk awareness into all core elements of the organisation, from C-level management through supervisors and department heads across the various supply chain functions
Timeframe	6 months (01.2010 – 07.2010)
Resources Required	Human Resources: SCRMT Monetary Resources (Budget): 5000 – 7500 €
Roles and Responsibilities	Have been determined

Table 15 continues on following page.

Table 15 continues as follows.

Additional Expertise Required	SCRM Consultant
Internal and external relationships	Other Departments (IT, Finance & Controlling, etc.) Major Customers – Key Supplier

Table 15 – Risk Management Context

4. Develop risk criteria

In this step, SCRMT has determined risk factors and their areas by the aid of developing the structure of the proposed framework which is illustrated and can be seen on Figure 24 below. Furthermore, after the determination of risk factors, the samples of those risk factors have also been found out by a comprehensive research of SCRMT.

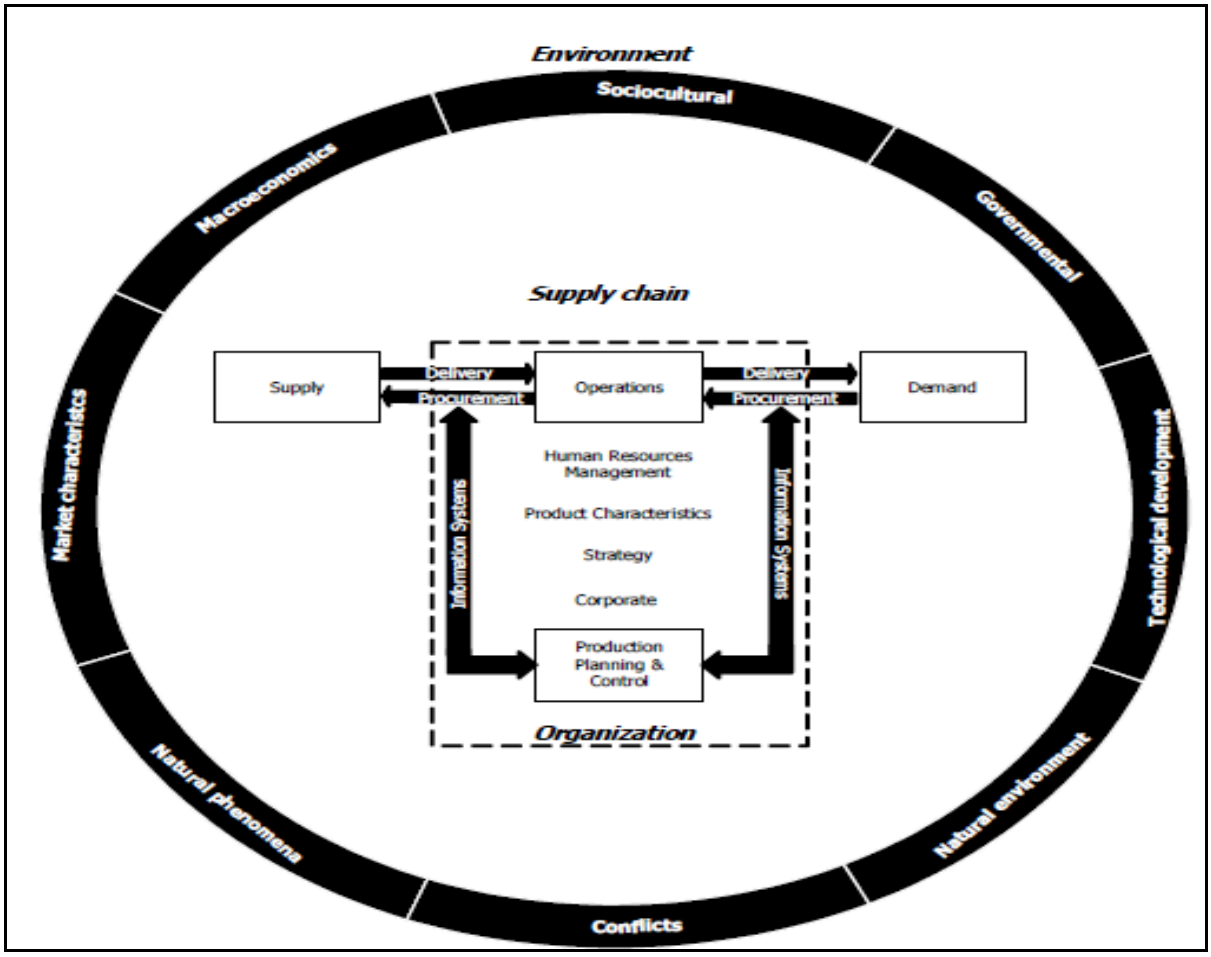


Figure 24 – the structure of the proposed Framework[133]

[133] Sami Kara, Berman Kayis, Emilie Gomez (2008), Volume 5, p. 105

Risk factors have been divided according to three main criterions. Those factors are basically classified as environmental, supply chain, and organisational factors. The risk areas and examples of these factors can be seen broadly on the following Tables. The first table is Table 16.

Risk Area	***Examples***
CONFLICT	*Coup d'état, terrorism, war*
GOVERNMENTAL	*Fiscal & Monetary reforms, government actions/policy, government change, inadequate provision of public services, legal risk (corporate social responsibilities), political stability, poor infrastructure, pressure group actions (non governmental groups or organisations), regulation (current & change), threat to government*
MACROECONOMICS	*Currency devaluation, economic activity, economic slump, economic stability, exchange rate, firms closing down, globalisation, inflation, level of trade barriers, multilateral agreements, price (control & change), terms of trade, unemployment rate*
MARKET CHARACTERISTICS	*Complementary goods availability, level of competition, market capacity, market stability, mass customisation, new entrants, new market opportunities, number of customers, number of qualified suppliers, raw material availability, speed of change, substitute goods availability*
NATURAL ENVIRONMENT	*Country's natural resources, disposal/recycling, environment preservation, global warming, natural resources depletion, pollution, waste generation*
NATURAL PHENOMENA	*Geological phenomenon, meteorological phenomenon*
SOCIO-CULTURAL	*Culture, demonstrations, labour dispute, labour unrest, riots, social concerns, social stability*
TECHNOLOGICAL DEVELOPMENT	*IT dependece, new technologies*

Table 16 - Sample of environmental factors[134]

[134] Sami Kara, Berman Kayis, Emilie Gomez (2008), Volume 5, pp. 106 - 107

On **Table 17**, the samples of supply chain factors can be seen.

Risk Area	***Examples***
DELIVERY	*Border crossing, damage in transit, delivery date, delivery failure (wrong location, time, quantity), handling, no incoming material, transportation lead time (delays), route (choice, change), transportation disruption, transportation modes (choice, change)*
DEMAND	*Change in customer tastes/needs, customer satisfaction, customers expand forecast, demand for performance, demand for variety, demand level, demand pattern regularity, demand predictability, demand volatility, loss of customer, service level*
INFORMATION SYSTEMS	*Incompatibility of information systems, information quality, information security, information sharing initiatives failure, information sharing systems implementation, information technology control failures, transaction complexity, transaction velocity*
PROCUREMENT	*Batch purchasing, bullwhip effect, erroneous order form, forward buying, procurement costs, product availability, purchasing cycles fluctuation*
RELATIONS	*Blurring boundaries, contracts, control, coordination, demand knowledge, dependence, inertia, information sharing, ownership, supply chain complexity, supply chain design, supply chain facilities, supply chain understanding, TQM program, trust, upstream company training in quality*
SUPPLY	*Financial stability, global sourcing, interruption of supply, obligation to the other customers, quality, sole sourcing, supplier location, supplier's flexibility, supplier's operations, supply lead time*

Table 17 - Sample of supply chain factors

On Table 18, the samples of organisational factors can be seen.

Risk Area	***Examples***
CORPORATE	*Claim to tribunal, compliance with regulatory environment, credit uncertainties, financial performance, fines, improper investments, loss of business, reputation, sales, taxes*
HUMAN RESOURCES MANAGEMENT	*Culture (resistance to change), employee availability, employee safety, key employee experience, managerial or employee self-interested behaviour, opportunistic behaviour, personnel reduction (lay off), reward for entrepreneurial risk taking, training programme*
OPERATIONS	*Accidents, adequate processes, asset impairment, automation, core competence, damage, defective product, destruction, equipment maintenance, equipment malfunctions, equipment obsolescence, flexibility, losses, production interruption, production lead time, production or technological change, productivity variation, quality consistency, rework*
PRODUCT CHARACTERISTICS	*Innovation, manufacturability, nature of product application, new product development, new product introduction, PLC, product variety, product/process complexity, product/process design change, time-to-market, uniqueness of product/process, unpredictable cycle times, use of common components*
PRODUCTION PLANNING AND CONTROL	*Buffer stock, capacity constraint, forecast accuracy, forecast horizon, forecasting difficulty, distortion, inventory control accuracy, inventory level, obsolescence rate, planning methods adequacy, replenishment lead time stability, scheduling methods, information adequacy, volume/mix requirement change*
STRATEGY	*Centralisation of production/distribution facilities, choice of partners, concurrent engineering, cost focus, focus on efficiency, focused factory, lack of mitigation & contingency plans, lean manufacturing, logistics conceptual choices (e.g. JIT), marketing strategies, objectives, outsourcing, pricing, quality focus*

Table 18 - Sample of organisational factors

5. Define the structure for risk analysis

SCRMT has prepared Supply Chain Risk Perspective of Anatolian Engineered Filters Ltd. in order to isolate the categories of risk that they aim to manage. This work will let SCRMT to identify significant supply chain related risks more deeply and accurately. Supply Chain Risk Perspective of the organisation has been depicted on Figure 25 as follows.

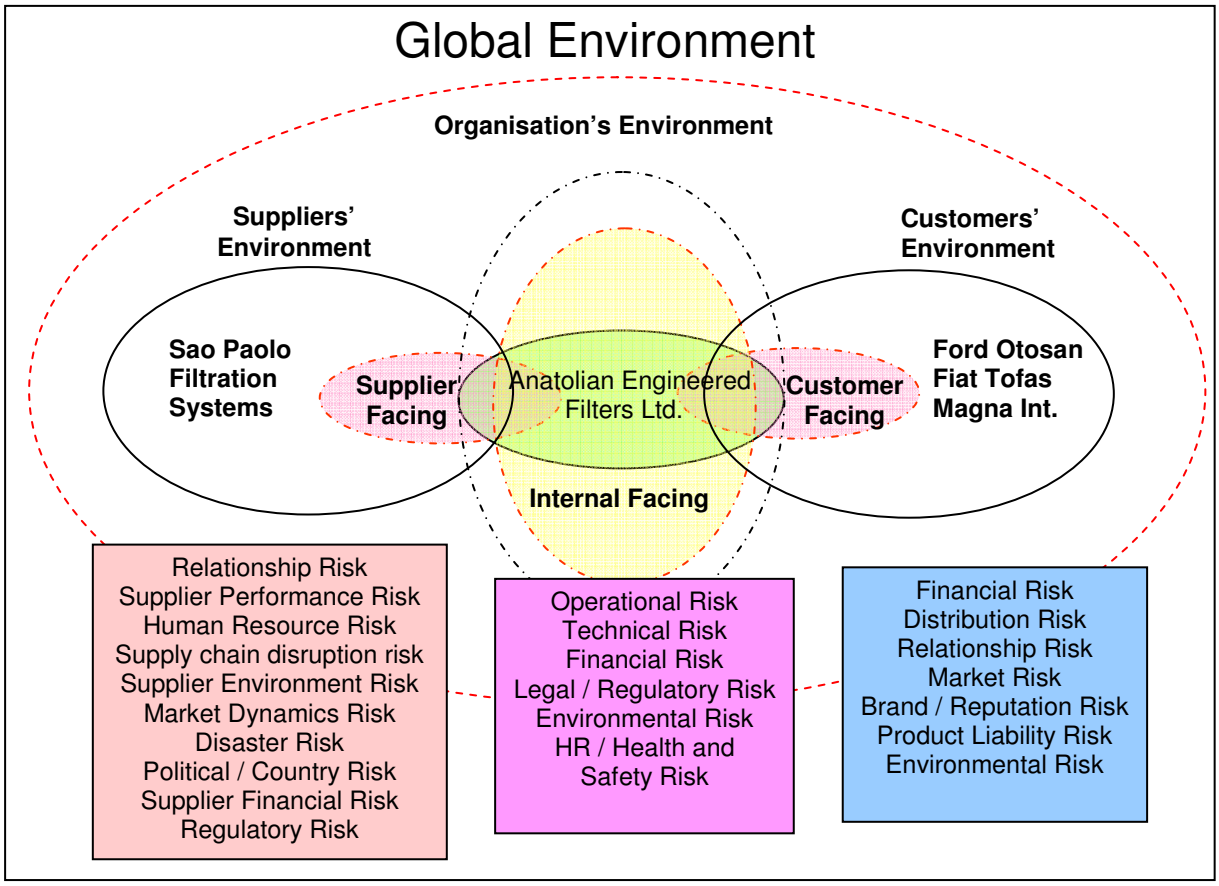


Figure 25 - Supply Chain Risk Perspective of Anatolian Engineered Filters Ltd.[135]

Once supply chain risk management context has been established entirely, the next duty of SCRMT was to identify risks. The risks that Anatolian Engineered Filters might face have been broadly identified by SCRMT of the organisations within the next chapter.

[135] Cf: Dave Morrow, Taylor Wilkerson, Melinda Davey (2009), p.13

5.4 Step 3: Identify the Risks

SCRMT has identified risks both retrospectively and prospectively. In order to achieve that, there are some sources of information and methods have been utilised to identify as many risks as possible. Some of those sources were:

- Hazard or incident logs or registers
- Customer complaints
- Accreditation documents and reports
- Past staff or client surveys
- Brainstorming with staff or external stakeholders
- Conducting interviews with relevant people and/or organisations
- Flow charting a process

Flow charting the process of the organisational Supply Chain Management has been specifically selected and worked on it to clearly see the possible risks and identify as much risks as possible. The flow chart has been illustrated as it is shown on **Figure 26**.

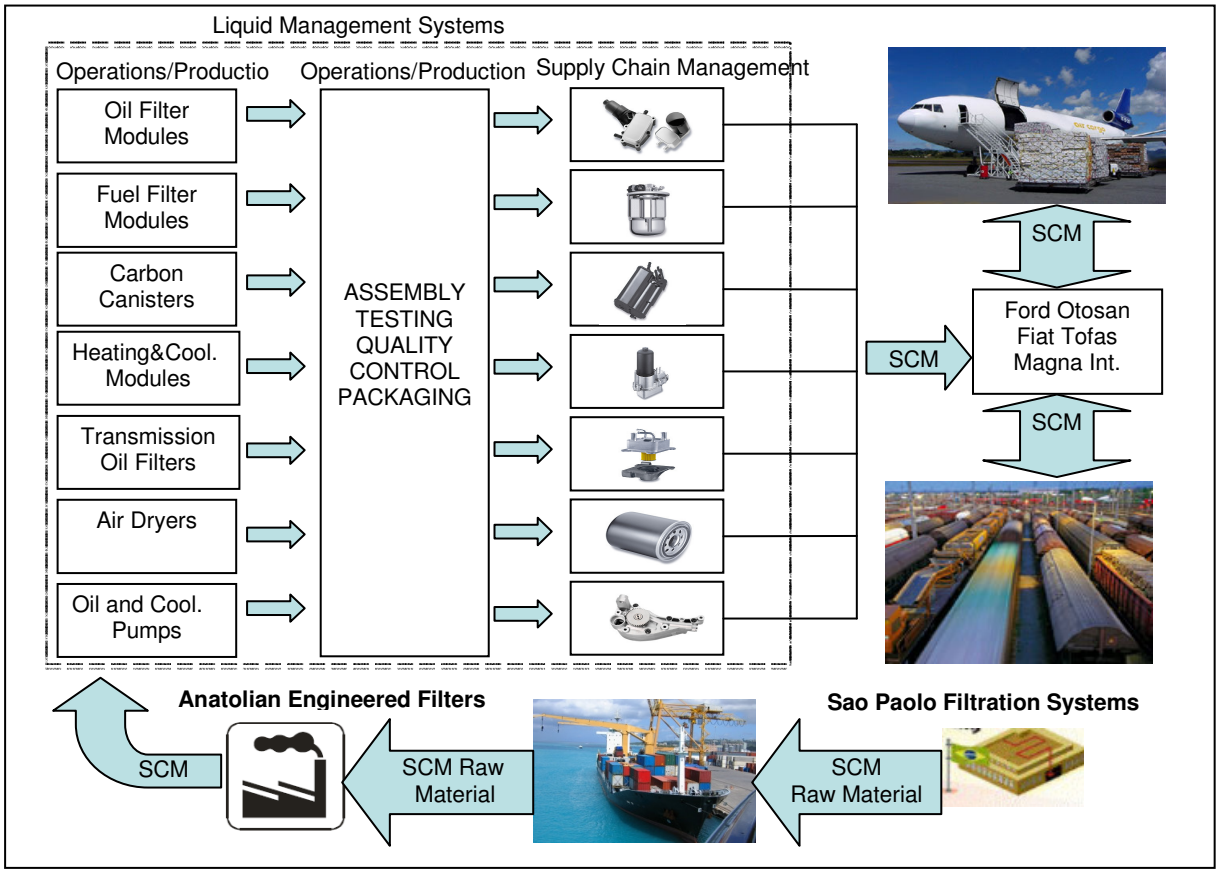


Figure 26 – Supply Chain Management Flow Chart of Anatolian Engineered Filters Ltd.

Furthermore, SCRMT has additionally prepared a Risk Identification Dashboard in order to determine and then focus on the specifically occurring risks. The Risk Identification Dashboard and risks that have been determined by SCRMT can be seen on following Table 19.

ID	Process Area	Risk Identification Dashboard	
		Event	Description
1	Source	Raw Material Supplier (Sao Paolo Filtration Systems) shut down by labour strike	The major raw material supplier from Brazil has been in talks and negotiations with their worker's union. The talks have been broken down and the union has gone on strike, shutting down all operations and shipments for 30 days
2	Plan	Out of stock with the distributors	The actual sales and distribution of Liquid Management Systems is 50% higher than forecast for domestic clients (Ford Otosan and Fiat Tofas). Distributors are out of stock leading to lost orders and emergency shipments from other regions. The Anatolian Engineered Filters Ltd. is on over time and it will take 30 days to catch up.
3	Make	Packaging Machine Failure	Products cannot be packaged automatically. Increase labour costs due to additional overtime to package the products manually
4	Deliver	Increased delivery costs due to high fuel price	Higher delivery costs from Anatolian Engineered Filters Ltd. to the customers resulting higher costs per unit. Loss of competitive advantage as the low cost Liquid Management Systems

Table 19 - Risk Identification Dashboard

Once risks have been determined by the aid of Risk Identification Dashboard, the next step taken was to analyse them. Risks have been analysed by SCRMT within the following chapter.

5.5 Step 4: Analyse the Risks

In this step, SCRMT has analysed above-determined risks by the aid of Risk Assessment Dashboard which has been combined with Risk Identification Dashboard. In addition to that, risks have been comprehensively analysed according to the annual probability, impact/consequence, and level of risk as well as total risk magnitude of them. The Risk Assessment Dashboard has been formed as it can be seen on Table 20 below.

ID	Process Area	Risk Identification	Risk Assessment			Risk Zone
		Event	Annual Probability (P)	Impact (I)	VAR P * I	
1	Source	Raw Material Supplier (Sao Paolo Filtration Systems) shut down by labour strike	10.0 %	4000 €	400 €	H
2	Plan	Out of stock with the distributors	20.0 %	1500 €	300 €	M
3	Make	Packaging Machine Failure	25.0 %	200 €	50 €	L
4	Deliver	Increased delivery costs due to high fuel price	60.0 %	500 €	300 €	M
TOTAL RISK MAGNITUDE (VAR) =						1050 €

Table 20 - Risk Assessment Dashboard

Note: All above-given costs are in '000 €

5.6 Step 5: Evaluate the Risks

Once risks have been analysed within the previous chapter, it is time to evaluate them by the aid of Risk Mitigation Dashboard that has been created by SCRMT in order to evaluate them quantitatively and find out some mitigation strategies. Those mitigation strategies have been showed on the Risk Mitigation Dashboard. Last but at least Total Mitigation Cost has been calculated according to inputs that can be seen on Risk Mitigation Dashboard. Risk Mitigation Dashboard can be seen on Table 21 below.

Note: All below-given costs are in '000 €

ID	Risk	Mitigation Strategy	Implement. Cost	New Prob. (P)	New Impact (I)	New VAR P * I	Original VAR	ROI
1	Raw Material Supplier (Sao Paolo Filtration Systems) shut down by labour strike	Determine suppliers which are unionised and consider the relationship among them. Need to certify back-up supplier and pay them an annual fee for stand by production capability.	40 €	10.0 %	1200 €	120 €	400 €	240 €
2	Out of stock with the distributors	Establish a central inventory at Anatolian Engineered Filters Ltd. Factory where is able to produce 2 weeks of 50% of demand for a region. Invite distributors to S&OP (Sales and Operations Planning) meetings.	100 €	5.0 %	600 €	30 €	300 €	170 €
3	Packaging Machine Failure	Maintain the machines frequently. Follow a schedule of machine retirement and replacement with new machines.	30 €	15.0%	20 €	3 €	50 €	17 €
4	Increased delivery costs due to high fuel price	Purchase and store back-up oil against an increase in fuel costs.	20 €	100 %	1 €	1 €	300 €	279 €
		TOTAL MITIGATION COST=	190 €			154 €	1050 €	706 €

Table 21 - Risk Mitigation Dashboard

5.7 Step 6: Treat the Risks

After risk evaluation has been done broadly by the aid of Risk Mitigation Dashboard, and risk mitigation strategies have been determined quantitatively afterwards. The next step that SCRMT would take was to treat risks which have been identified within the previous steps. This step has been explained and investigated deeply by the aid of a Risk Mitigation – Action Plan Dashboard that has been formed by SCRMT. The mitigation actions, responsible person who was in charge to take the mitigation action, status of these actions, and deadline of mitigation action have been shown on Risk Mitigation – Action Plan Dashboard. Risk Mitigation – Action Plan Dashboard has been illustrated on following Table 22.

ID	Mitigation Action	Responsible Person	Status	Deadline	Risks Addressed
1	Determine suppliers which are unionised and consider the relationship among them. Need to certify back-up supplier and pay them an annual fee for stand by production capability.	Risk Officer from Supply Chain Management and SCRM Consultant	Suppliers identified Annual fee to be negotiated	End of 03.2010	Raw Material Supplier (Sao Paolo Filtration Systems) shut down by labour strike
2	Establish a central inventory at Anatolian Engineered Filters Ltd. Factory where is able to produce 2 weeks of 50% of demand for a region. Invite distributors to S&OP (Sales and Operations Planning) meetings.	Risk Officers from Operations/Production, Supply Chain Management and Sales and Marketing	New inventory level defined for the products	Done	Out of stock with the distributors
3	Maintain the machines frequently. Follow a schedule of machine retirement and replacement with new machines.	Head of Engineering and Maintenance Department	In Progress	Immediately	Packaging Machine Failure
4	Purchase and store back-up oil against an increase in fuel costs.	Risk Officers from Finance & Controlling, Supply Chain Management and SCRM Consultant	Risk Officer from Finance & Controlling has been assigned to be responsible person for mitigation action	End of 05.2010	Increased delivery costs due to high fuel price

Table 22 – Risk Mitigation – Action Plan Dashboard

5.8 Step 7: Monitoring and Review

This step has been executed by the cooperation among SCRMT and Internal Audit Department whose responsibilities have been determined on Table 23 below:

Internal Audit Department	• Makes formal assessments of Supply Chain Risk Management Implementation in areas of concern. • Assesses the controls in place to manage, mitigate or reduce supply chain related risks. • Execute monitoring and reviewing process and report necessary actions concerning those issues where it is required. • Manage internal audit events and cooperate closely with SCRMT during the implementation process.

Table 23 - Internal Audit Department

5.9 Summary

After the entire SCRM Implementation has been achieved, SCRMT evaluated the implementation results and presented them to the Board. SCRMT has evaluated each risk that they found out and showed on Risk Identification Dashboard. The evaluation and results of SCRM Implementation have been given as follows:

1) Process Area: Source

The results can be seen on Figure 27 below.

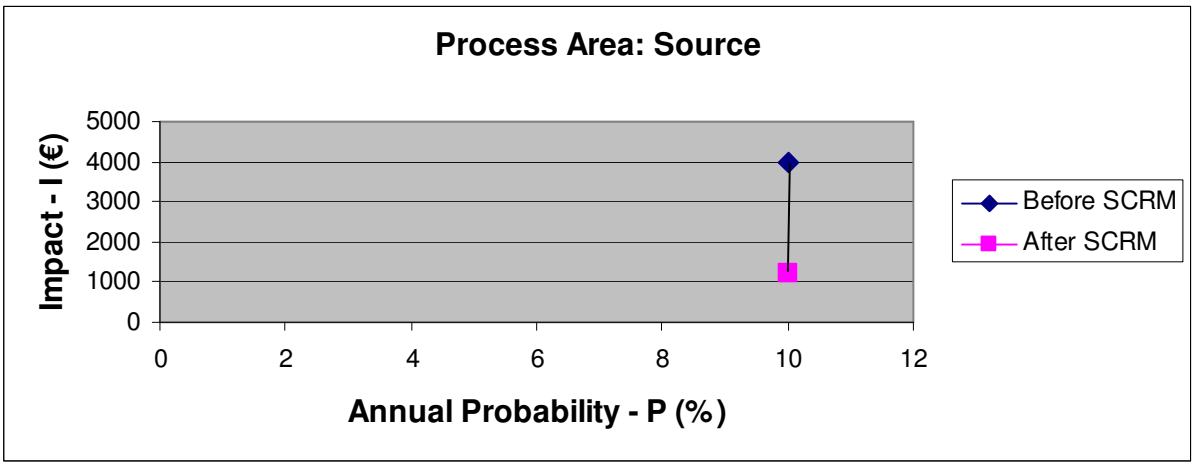


Figure 27 - Process Area: Source

Note: All above-given costs are in '000 €

As it is seen on Figure 27 above, on the one hand, the annual probability of risk remained the same percentage (10%), after the mitigation action has been taken that has been mentioned on Table 22 before. On the other hand, the impact of the risk has been reduced from 4000 € to 1200 € which means the mitigation action reduced the impact of risk by 70 %, after it has been taken.

2) Process Area: Plan

The results can be seen on Figure 28 below.

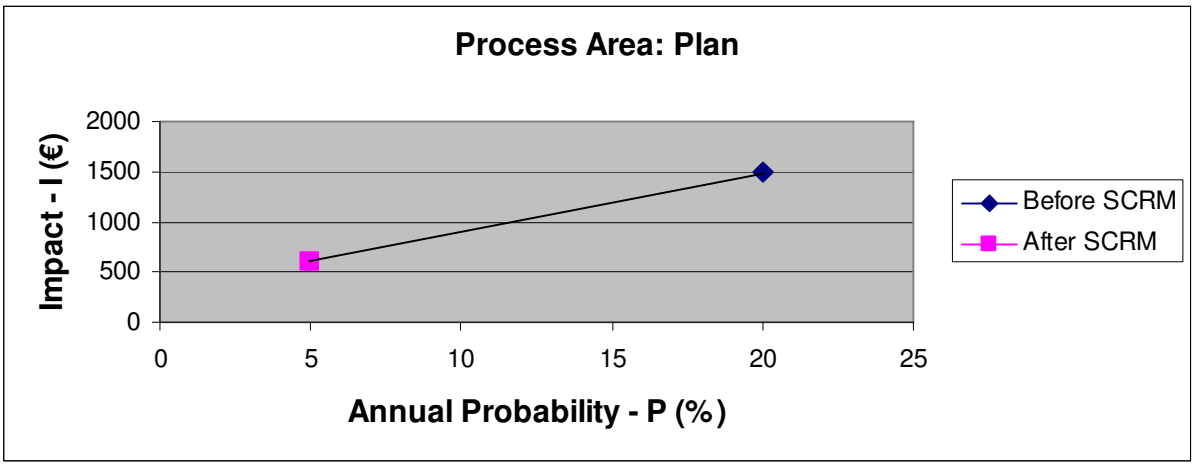


Figure 28 - Process Area: Plan

Note: All above-given costs are in '000 €

As it is seen on Figure 28 above, the annual probability of risk has been reduced from 20 % to 5 % that means the mitigation action that has been mentioned on Table 22 before reduced the annual probability of risk by 75 %. Conversely, the impact of the risk has been reduced from 1500 € to 600 € which means the mitigation action reduced the impact of risk by 60 %, after it has been taken.

3) Process Area: Make

The results can be seen on Figure 29 below.

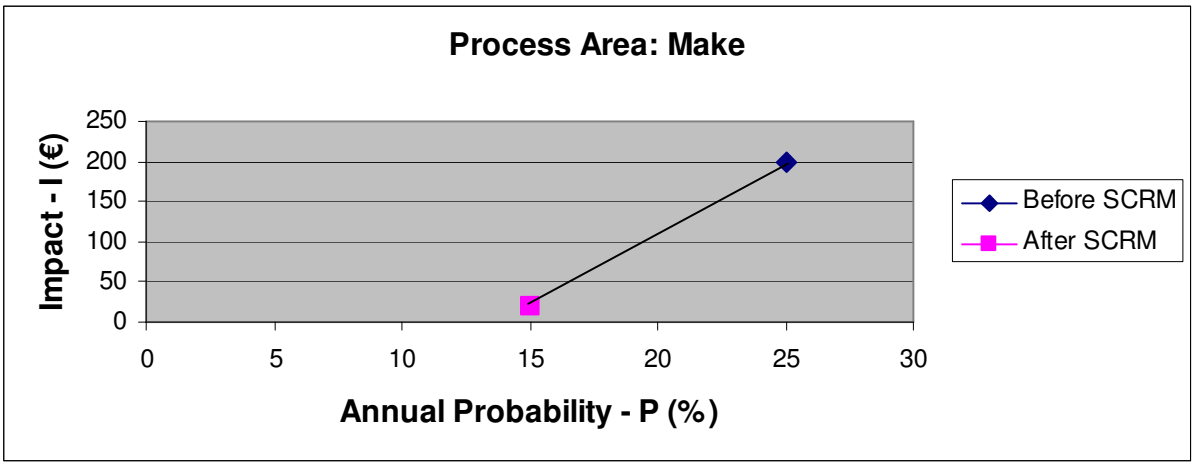


Figure 29 - Process Area: Make

Note: All above-given costs are in '000 €

As it is seen on Figure 29 above, the annual probability of risk has been reduced from 25 % to 15 % that means the mitigation action that has been mentioned on Table 22 before reduced the annual probability of risk by 40 %. Conversely, the impact of the risk has been reduced from 200 € to 20 € which means the mitigation action reduced the impact of risk by 90 %, after it has been taken.

4) Process Area: Deliver

The results can be seen on Figure 30 below.

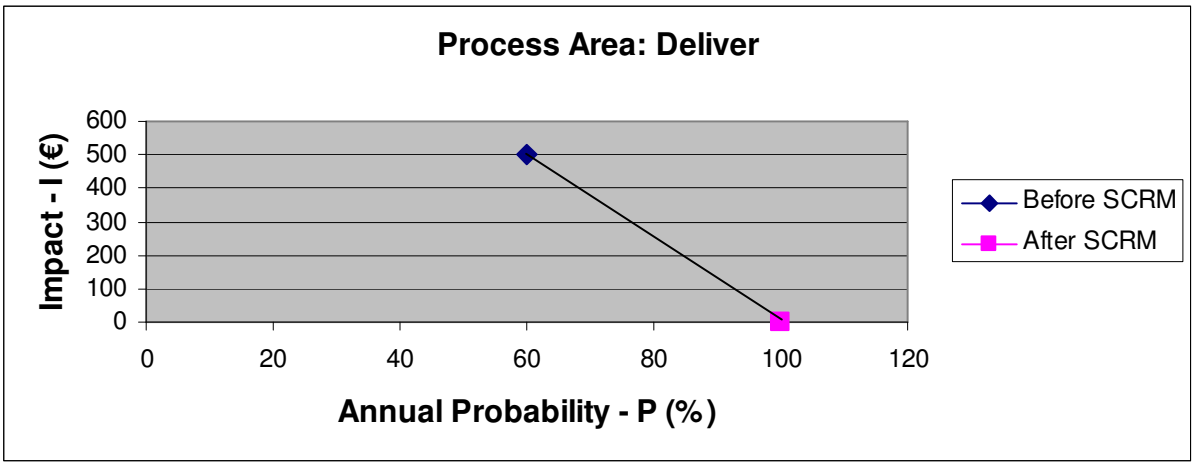


Figure 30 - Process Area: Deliver

Note: All above-given costs are in '000 €

As it is seen on Figure 30 above, on the one hand, the annual probability of risk has been increased from 60 % to 100 % that means the mitigation action that has been mentioned on Table 22 before raised the annual probability of risk by 66, 6 %. Conversely, the impact of the risk has been reduced from 500 € to 1 € which means the mitigation action reduced the impact of risk by 99, 8 %, after it has been taken.

6. CONCLUSION

The globalisation plays a crucial role and it is becoming the major concern of economies in present-day business world whose complexity is continually increasing. Therefore, organisations which aim to broad the horizon of their vision in order to stay on the market are motivated and willing to pay more attention to competitive new management approaches like Risk Management, Operational Risk Management (ORM) and etc.

In addition to that, an effectively implemented Operational Risk Management provides a sustainable framework that clearly identifies, analyses the potential threats and opportunities, and deals with them properly by avoiding or mitigating errors. If we talk about risks regarding inadequate or failed internal processes, people and systems, or external events, then an effective ORM should be implemented appropriately in order to manage those risks.

Moreover, the business advantages of an effective ORM are obvious to be taken. Some of these benefits can be summarised as follows:

- Making everybody “Risk Manager” within the organisation by creating a Risk Management Culture that provides a vision to all staff to understand the root causes of risks, and their responsibility to avoid or mitigate them.
- Keeping the awareness and perception of all kind of risks throughout the organisation by permanently communicating, reviewing and monitoring all risks the organisation faces.
- Taking the competitive advantage to lead the industry by reducing the operational mishaps and business disruptions that are caused by operational risks.
- Expanding customer portfolio, shareholder confidence and protecting organisational reputation by keeping organisational success stable and continuously improving operational performance and efficiency.
- Gaining full satisfaction of customers by being more flexible and response quicker to their continually changing needs.
- Managing changes more effectively and efficiently and thus providing business continuity by successful combination of Change Management applications and Operational Risk Management approach.

- Gaining full satisfaction of all employees, shareholders, stakeholders, the authorities and other communities, and thus creating value by providing better understanding of compliance with, legal and regulatory requirements, corporate culture and ethical requirements.
- …

Last but not least, the organisations that aim to take competitive advantage should take ORM as serious as other management disciplines. The organisations should not consider ORM as an additional expense. Conversely, they should recognise it as an opportunity to improve their business by more effective people, processes, and systems which are being appreciated and rewarded by customers, and shareholders.

LIST OF FIGURES

LIST OF TABLES

LIST OF REFERENCES

ACCENTURE, “Managing Risks for High Performance in Extraordinary Times, Report on the Accenture 2009 Global Risk Management Study”, 2009, Page 18, Available from: http://www.accenture.com/NR/rdonlyres/78589759-FE29-43E3-AFDF171D1B9F2587/0/Accenture_Managing_Risk_for_High_Performance_in_Extraordinary_Times.PDF (Consulted on 01.09.2009)

ANAND SUBRAMANIAM, “Supply Chain Risk Management, Minimising Risk Exposure in Supply Chain”, 2009, Page 15, Available from: http://www.slideshare.net/anandsubramaniam/supply-chain-risk-management (Consulted on 12.12.2009)

AUSTRALIAN CAPITAL TERRITORY PROCUREMENT CIRCULAR, “Risk Management”, May 2009, Page 2, Available from: http://www.procurement.act.gov.au/__data/assets/pdf_file/0010/57439/2009_24_Risk_Management.pdf (Consulted on 07.08.2009)

AUSTRALIAN CAPITAL TERRITORY PROCUREMENT CIRCULAR, “Risk Management”, May 2009, Page 5, Available from: http://www.procurement.act.gov.au/__data/assets/pdf_file/0010/57439/2009_24_Risk_Management.pdf and www.finance.gov.au/.../Table_Qualitative_Risk_Analysis_Matrix.rtf, (Consulted on 14.08.2009)

AUSTRALIAN GOVERNMENT – DEPARTMENT OF DEFENCE, “Example of Qualitative Risk Analysis Matrix”, 2009, Available from: http://www.defence.gov.au/ARMY/PUBS/Tramm/Volume%202/Section%201/V2-S1-C2-AB.pdf (Consulted on 07.10.2009)

AUSTRALIAN/NEW ZEALAND RISK MANAGEMENT STANDARD, “AS/NZS 4360:2004”, page 39, and AUSTRALIAN AGENCY FOR INTERNATIONAL DEVELOPMENT (AusGuideline), page 5, Available from: http://www.ausaid.gov.au/ausguide/pdf/ausguideline6.3.pdf - http://pandora.nla.gov.au/pan/54643/20051206-0000/www.smallbiz.nsw.gov.au/NR/rdonlyres/57688513-FCF3-4AF4-AC76-B2B640974C10/0/RiskManagementfullcopy.pdf (Consulted on 05.08.2009)

AVNER BARNEA, “Using the McKinsey’s 7-S Model to Improve Competitive Intelligence Capabilities”, May-June 2008, Volume 11, Number 3, page 51-52, Available from: http://www.scribd.com/doc/3115236/Using-the-McKinsey-7S-Model-to-Improve-Competitive-Intelligence-Capabilities (Consulted on 10.11.2009)

BRITISH STANDARDS INSTITUTION, “Risk Management Code of Practice”, October 2008, Available from: http://www.talkingbusinesscontinuity.com/useful-documentation/bs-31100-2008-risk-management-code-of-practice.aspx (Consulted on 27.08.2009)

BRITISH TELECOMMUNICATIONS, "Unlocking business value from effective operational risk management", 2005, Page 2, Available from: http://globalservices.bt.com/static/assets/pdf/brochures/security_compliance_26_orm_ferit_21sep_unlocking_business_value_from_effective_operational_risk_management.pdf (Consulted on 01.09.2009)

BRONWYN FRIDAY, "Risk Management in Practice: Adding value through ERM", 15 March 2006, Available from: http://www.riskmanagementmagazine.com.au/articles/F6/0C03DBF6.asp?Type=125&Category=1239 (Consulted on 12.11.2009)

BRUCE MCDOUGALL, "President Brucer Media Inc. Canada", 08 July 2009 Available from: http://www.mckinseyquarterly.com/Peter_L_Bernstein_on_risk_2211 (Consulted on 02.08.2009)

BY KUTENK, "Different Types of Risks, Operational Risk, Strategic Business Risk, Reputational Risk", 10 July 2009, Available from: http://www.kutenk.com/2009/07/10/different-types-of-risk-operational-risk-strategic-business-risk-reputational-risk/ (Consulted on 29.08.2009 - 30.08.2009)

BY KYLE, "R.I.P Peter L. Bernstein – Father of Risk", 27 July 2009, Available from: http://amateurassetallocator.com/2009/07/27/rip-peter-l-bernstein-father-of-risk/ (Consulted on 02.08.2009)

CRAIG BORYSOWICH, "Observation from a Tech Architect: Enterprise Implementation Issues & Solutions", 25 September 2007, Available from: http://it.toolbox.com/blogs/enterprise-solutions/managing-buyin-risk-management-checklist-19309 (Consulted on 17.11.2009)

DAVE MORROW, TAYLOR WILKERSON, MELINDA DAVEY, "Managing Risk in your organisation with the SCOR Methodology, Supply Chain Council Inc.", 20 February 2009, Page 13 - 22, Available from: https://www.supply-chain.org/node/1924

DAVID HAKALA, "The Top 10 Leadership Qualities", 19 March 2008, Available from: http://www.hrworld.com/features/top-10-leadership-qualities-031908/ (Consulted on 09.10.2009)

DELOITTE FINANCIAL SERVICES, "Risk Management Implementation: buy-side challenges and solutions", June 2008, Page 2 - 4, Available from: http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/us_fsi_FF_buy-side_june08.pdf (Consulted on 22.11.2009)

DIPL. – ING. DR. TECHN. WERNER LEITNER, DIPL. ING. VLADIMIR VALASTIAK, "Quality Management Course Script", 2nd Edition 2009-2010, Introduction page 4, Graz University of Technology

DONALD ESPERSEN, “The language of risk: organisations can improve risk management and audit processes by communicating risks in terms that everyone understands”, June 2007, Page 1-2, Available from: http://findarticles.com/p/articles/mi_m4153/is_3_64/ai_n19328590/pg_2/?tag=content;col1 (Consulted on 15.11.2009)

DOUGLAS G. HOFFMAN, “Managing Operational Risk, 20 Firm-wide Best Practice Strategies”, 11 January 2002, Page 51 (Consulted on 02.11.2009)

DOUGLAS W. HUBBARD, “The Failure of Risk Management: Why It's Broken and How to Fix It”, 27 April 2009, Chapter 2 p.27, Chapter 3 p.46, Available from: http://en.wikipedia.org/wiki/Risk_management and http://books.google.com/books?id=e0IoQJcn1-YC&printsec=frontcover&dq=Douglas+Hubbard&lr=&hl=tr#v=onepage&q=&f=false (Consulted on 02.08.2009 – 19.08.2009)

ERNST & YOUNG, “Speed through common language – Critical Factors in Risk Management today”, 2009, Page 1-3, Available from: http://www.iia.nl/SiteFiles/Downloads/Ernst%20%20Young%20-%20Speed%20Through%20Common%20Language%20-%20Critical%20factors%20in%20risk%20management%20today%20-%20June%202009.pdf (Consulted on 15.11.2009)

ERNST & YOUNG IN COLLABORATION WITH OXFORD ANALYTICA, “The 2009 Ernst & Young business risk report – the top 10 risks for global business”, 2009, Page 3-4, Available from: http://www.ey.com/Global/assets.nsf/International/2009_business_risk_report/$file/2009_business_risk_report.pdf (Consulted on 23.08.2009)

FEDERAL AVIATION ADMINISTRATION (FAA), “System Safety Handbook Chapter 15: Operational Risk Management”, 3 December 2000, Page 3, Available from: http://www.faa.gov/library/manuals/aviation/risk_management/ss_handbook/media/chap15_1200.pdf (Consulted on 08.10.2009)

FRESHPATENTS.COM, “Semi quantitative Risk Analysis”, November 2007, Available from: http://www.freshpatents.com/Semi-quantitative-risk-analysis-dt20071122ptan20070271198.php, (Consulted on 15.08.2009)

GLOBAL RISK ALLIANCE PTY. LTD. jointly with NEW SOUTH WALES (AUSTRALIA) DEPARTMENT OF STATE AND REGIONAL DEVELOPMENT, “Risk Management Guide for small business”, May 2005, Page 22 – 38, Available from: http://pandora.nla.gov.au/pan/54643/20051206-0000/www.smallbiz.nsw.gov.au/NR/rdonlyres/57688513-FCF3-4AF4-AC76-B2B640974C10/0/RiskManagementfullcopy.pdf, (Consulted on 06.08.2009)

HONGYI SUN, IP KEE HUI, AGNES Y.K. TAM, JAN FRICK, “Employee Involvement and Quality Management”, 2000, Volume 12, Issue 5, Page 350-354, Available from: http://www.emeraldinsight.com/fig/1060120506003.png, (Consulted on 14.10.2009)

INTERNATIONAL CIVIL AVIATION ORGANISATION (ICAO), "Safety Management Manual", First Edition-2006, Page 16-17, Available from: http://www.icao.int/fsix/_Library/SMM-9859_1ed_en.pdf (Consulted on 07.10.2009)

INTERNATIONAL JOURNAL OF PHYSICAL DISTRIBUTION & LOGISTICS, "Ericsson's proactive supply chain risk management approach after a serious sub-supplier accident", Page 5, and WORAPHAN ATIKOMRITAT, "Hewlett-Packard Supply Chain Management", page 3, and ROBERT J. SCHNEIDER, "Supply Chain Risk Management Risk in the evolving supply chain process", 27 October 2008, page 2, Available from: http://www.slideshare.net/tung148/hp-supply-chain, , (http://www.industryweek.com/articles/supply_chain_risk_management_17614.aspx?Page=2) (Consulted on 15.12.2009)

INTERNET ENCYCLOPEDIA OF PHILOSOPHY, Available from: http://www.iep.utm.edu/yinyang/ (Consulted on 07.11.2009)

INVESTOPEDIA.COM "Management buy-in (MBI)", 2009, Available from: http://www.investopedia.com/terms/m/mbi.asp (Consulted on 17.11.2009)

JAMES LAM, "Enterprise-wide Risk Management and the role of the chief risk officer", 25 March 2000, page 4, Available from: http://www.erisk.com/Learning/Research/011_lamriskoff.pdf (Consulted on 03.12.2009)

JAMES LAM, "Operational Risk Management – Beyond Compliance to Value Creation", June 2007, page 10, Available from: http://www.jameslam.com/media/OpenPages%20ORM%20White%20Paper_June%202007.pdf , (Consulted on 04.11.2009)

JAMES LAM, "Top ten requirements of Operational Risk Management", 01 November 2001, Available from: http://www.erisk.com/About/PressRoom/TopTenRequirementsofOpera.asp, (Consulted on 03.11.2009 – 06.11.2009)

JAMES LAM, "Enterprise Risk Management, PRMIA Boston Chapter Meeting", 29 April 2008, page 7, Available from: http://www.prmia.org/Chapter_Pages/Data/Files/2375_3009_ERM%20042908_Lam_presentation.pdf (Consulted on 03.12.2009)

JAMES L. VESPER, "Risk Assessment and Risk Management in the Pharmaceutical Industry: Clear and Simple", 2006, Chapter 1, Page 1, 8, Available from: https://store.pda.org/bookstore/TableOfContents/Risk_Assessment_Ch01.pdf (Consulted on 01.08.2009)

JASON BATMAN, "Qualitative Risk Analysis (QRA)", 23 January 2009, Page 1, Available from: http://www.docstoc.com/docs/3742205/Quantitative-Risk-Analysis-(QRA) (Consulted on 15.08.2009)

KEVIN W. KNIGHT, “Resolving Challenges to Implementing Risk Management”, 17 June 2003, page 16, 17, 19, 22, 31, 36, 37, 41 Available from: http://www.tbs-sct.gc.ca/rm-gr/international/pp/challngs-écueils_e.pdf (Consulted on 10.11.2009 - 04.12.2009)

LLOYDS.COM, “The Chief Risk Officers are coming”, 31 July 2009, Available from: http://www.lloyds.com/News_Centre/Features_from_Lloyds/News_and_features_2009/360/The+chief+risk+officers+are+coming.htm (Consulted on 03.12.2009)

MICHEL CROUHY, DAN GALAI, ROBERT MARK, “The Essentials of Risk Management”, 2006, Chapter 13, Page 332 (Consulted on 02.11.2009)

MIKE WILKINSON, “The role of technology in risk management, EMB Risk Management Consulting”, 2009, Page 2, Available from: http://www.emb.com/EMBDOTCOM/UK/UK/Resources/EMB%20Briefings_technology_risk%20management.pdf (Consulted on 22.11.2009)

MUSTAFA GÜLTEKIN, “Professor University of North Carolina Chapel Hill, NC/USA”, 09 July 2009, Available from: http://www.mckinseyquarterly.com/Peter_L_Bernstein_on_risk_2211 (Consulted on 02.08.2009)

NOREEN FOH, “Control Self-Assessment: A new approach to auditing”, September/October 2000, page 1, Available from: http://www.iveybusinessjournal.com/view_article.asp?intArticle_ID=249 (Consulted on 18.11.2009)

NORTH CAROLINA (NC) STATE UNIVERSITY, “ERM: The importance of Senior Management Buy-in and Leadership”, 01 May 2008, Available from: http://www.mgt.ncsu.edu/erm/index.php/articles/entry/csuite-buy-in/ (Consulted on 17.11.2009)

OFFICE OF GOVERNMENT COMMERCE (OGC), “Management of Risk: Guidance for Practitioners”, 2007, Page 62, (Consulted on 04.12.2009)

OXFORD ENGLISH DICTIONARY, and DAVID A. AAKER, “Harvard Business Publishing Marketing in a Silo World: The New CMO Challenge”, 01 November 2008, Available from: http://www.askoxford.com/concise_oed/silo?view=uk http://harvardbusiness.org/product/marketing-in-a-silo-world-the-new-cmo-challenge/an/CMR415-PDF-ENG (Consulted on 04.11.2009)

PATRICK OW, “Victorian Managed Insurance Authority (VMIA) Draft ISO 31000:2009 Risk Management - Principles and Guidelines”, June 2009, Page 5-6, Available from: http://www.vmia.vic.gov.au/skillsEDIT/clientuploads/48/Introduction%20to%20ISO31000%20June%202009.pdf (Consulted on 05.08.2009)

PETER L. BERNSTEIN, “The Measure of Our Ignorance” from “AGAINST THE GODS”, 1998, Page 197, Available from: http://www.peterbernstein.com/peters_books_against.htm (Consulted on 02.08.2009)

PREETAM KAUSHIK, “Qualitative and Quantitative Risk Analysis”, 29 April 2009, Available from: http://www.brighthub.com/office/project-management/articles/33403.aspx , (Consulted on 15.08.2009)

PRICEWATERHOUSECOOPERS HONG KONG, “Internal Audit – Risk / Control Self Assessment”, 2002, Available from: http://www.pwchk.com/home/eng/ia_risk.html (Consulted on 18.11.2009)

PROF. MOHAMMAD MODARRES, “Risk Analysis in Engineering: techniques, tools, and trends”, 13 January 2006, Volume 174, Page 6, Available from: http://books.google.com/books?id=ErjFzRWSne8C&printsec=frontcover&hl=tr&source=gbs_navlinks_s#v=onepage&q=&f=false (Consulted on 15.08.2009)

PUBLIC SAFETY CANADA, “A guide to business continuity planning”, 21 January 2009, Available from: http://www.publicsafety.gc.ca/prg/em/gds/bcp-eng.aspx#top_of_page, (Consulted on 19.08.2009)

QUUENSLAND GOVERNMENT – ENVIRONMENT AND RESOURCE MANAGEMENT, “Guidelines for Implementing Total Management Planning”, 2008, page 10, Available from: http://www.nrw.qld.gov.au/compliance/wic/pdf/guidelines/tmp/2001_guidelines/implementation/risk_1.pdf, (Consulted on 16.08.2009)

RITA MULCAHY, “Risk Management Tricks of the Trade for Project Managers”, 2003, Chapter 7, Page 158-159 (Consulted on 02.11.2009)

ROADSIDEAMERICA.COM, “The Pepsi Product Tampering Scandal of 1993”, 17 December 2009, Available from: http://www.roadsideamerica.com/rant/pepsipanic.html (Consulted on 07.10.2009)

ROBERT SEMKE, “Operational Risk Management, An Element of Enterprise Risk Management at Metlife”, 2006, Page 5, Available from: http://www.ermsymposium.org/2006/pdf/handouts/RCM/RCM5_Rsemke.pdf (Consulted on 03.11.2009)

SAMI KARA, BERMAN KAYIS, EMILIE GOMEZ, “Managing Supply Chain Risks in Multi-Site, Multi-partner Engineering Projects, School of Mechanical and Manufacturing, The University of New South Wales, Sydney/Australia”, 2008, Volume 5, page 105 - 107, Available from: http://www.ibima.org/pub/journals/CIBIMA/volume5/v5n14.pdf (Consulted on 19.12.2009)

STUART FAGG, “In the Loop: Risk Reporting, Risk Management Magazine”, 22 November 2009, Available from: http://www.riskmanagementmagazine.com.au/articles/38/0C04E738.asp?Type=124&Category=1240 (Consulted on 21.11.2009)

SUSAN M. HEATHFIELD, “Human Resources, Employee Involvement, Definition and Examples”, Available from: http://humanresources.about.com/od/glossarye/a/employee_inv.htm (Consulted on 14.10.209)

THITIMA PITINANONDHA, “Operational Risk Management (ORM) Systems an Australian Study”, June 2008, Page 2, 36 - 43 Available from: http://epress.lib.uts.edu.au/dspace/bitstream/2100/600/2/02.whole.pdf (Consulted on 29.08.2009)

TIM CREASEY, “Defining change management”, 23 September 2009, Available from: http://www.change-management.com/tutorial-definition-2009.htm (Consulted on 10.11.2009)

THE STATE OF QUEENSLAND – DEPARTMENT OF EDUCATION AND TRAINING, 2006, Available from: http://education.qld.gov.au/riskmanagement/treat.html (Consulted on 28.08.2009)

THE STATE OF QUEENSLAND - PROPERTY MANAGEMENT COMMITTEE “Asset Management Knowledge Centre, Risk Management Context”, 2009, Available from: http://www.pmc.qld.gov.au/knowledge/policy/asset/risk/context_risk.php (Consulted on 08.08.2009)

THE YING AND YANG, Available from: http://halfbit.org/logos/ying-yang.jpg (Consulted on 07.11.2009)

UNIVERSITY OF EXETER/UK, “Centre for Leadership Studies, Leadership Definitions”, Available from: http://www.leadership-studies.com/lsw/definitions.htm, (Consulted on 09.10.2009)

U.S. NAVAL SAFETY CENTRE, “ORM Downloadable Resources, Introduction to ORM”, February 2009, Page 2, Available from: http://www.safetycenter.navy.mil/ORM/downloads/index.asp (Consulted on 29.08.2009)

U.S. NAVAL SAFETY CENTRE, “4 Principles of Applying ORM”, Available from:http://www.safetycenter.navy.mil/orm/generalorm/introduction/4principles.htm (Consulted on 09.10.2009)

VICTORIAN MANAGED INSURANCE AUTHORITY (VMIA), “Risk Insight - Risk Report Summaries”, January/June 2009, Page 8, Available from: http://www.vmia.vic.gov.au/skillsEDIT/clientuploads/48/0609%20Risk%20Report%20Summaries%20Final%20250609_1.pdf (Consulted on 01.09.2009)

VICTORIAN MANAGED INSURANCE AUTHORITY (VMIA), “Strategic and Operational Risk Management”, 2009, Available from: http://www.vmia.vic.gov.au/display.asp?entityid=5536 (Consulted on 05.08.2009)

VIKRAM S. TYAGI, “Logistics & Supply Chain Management”, 2007, page 14, Available from: http://www.slideshare.net/chinu/introduction-to-supply-chain-management (Consulted on 15.12.2009)

WIKIPEDIA – “Contingency Plan”, 21 May 2009, Available from: http://en.wikipedia.org/wiki/Contingency_plan, (Consulted on 20.08.2009)

WIKIPEDIA – “Crisis Management”, 06 October 2009, Available from: http://en.wikipedia.org/wiki/Crisis_management (Consulted on 07.10.2009)

WIKIPEDIA – “Risk”, Available from: http://en.wikipedia.org/wiki/Risk (Consulted on 25.07.2009)

WIKIPEDIA – “Operational Risk”, 22 August 2009, Available from: http://en.wikipedia.org/wiki/Operational_risk (Consulted on 29.08.2009)

WOLFGANG KERSTEN, PHILIPP HONRATH & MAIREKE BÖGER, “An Empirical Approach to Supply Chain Risk Management: Development of a Strategic Framework, Hamburg University of Technology”, 2007, Page 11, Available from: http://www.poms.org/conferences/poms2007/cdprogram/Topics/full_length_papers_files/007-0507.pdf (Consulted on 06.12.2009)

WORCESTERSHIRE HEALTH SERVICES/UK, “Risk Analysis Matrix”, Available from: http://www.worcestershirehealth.nhs.uk/EXTRANET_Library/LINDAMARRIOTT/Risk%20Analysis%20Matrix%20revised%202.pdf (Consulted on 07.10.2009)