UNIVERSITY OF TAMPERE
School of Management

THE USE OF THE RISK MANAGEMENT STANDARD ISO 31000 IN FINNISH ORGANIZATIONS

Insurance Science
Master's Thesis
December 2012
Author: Aleksi Liuksiala
Supervisor: Olli-Pekka Ruuskanen

ABSTRACT

University of Tampere	School of Management, Insurance Science
Author:	LIUKSIALA, OSKAR ALEKSI

Title:	The use of the risk management standard ISO 31000 in Finnish organizations
Master's thesis:	87 pages, 3 appendix pages
Date:	December 2012
Key words:	Risk management, ISO 31000, Enterprise Risk Management, ERM

The requirements for effective risk management have grown during the recent years. The first decade of the current millennium has seen a number of economic crises, beginning from the collapse of Enron in 2001 to the latest capital market crisis in 2008, which have been drivers for increased corporate governance. The globally interconnected economy calls for heightened awareness of the uncertainty factors related to the operational environment. As a response to these emerging needs, a substantial growth and development has been seen in the risk management industry. However, the diversity of different actors in the field of risk management has been a source for much confusion and ambiguity with regard to mutual RM practices and the use of terminology. The attempts to harmonize risk management practices have been actualized in a number of risk management standards, latest of which is ISO 31000. The new risk management standard is anticipated to achieve the position as a global benchmark for risk management practices.

This study attempts to examine the use of the risk management standard ISO 31000 in Finnish organizations. The main emphasis is in measuring the performance of risk management against the requirements of the standard. To address this issue, a survey was conducted to Finnish risk management professionals representing enterprises and public sector organizations. In addition to investigating the current use of ISO 31000, the survey investigated the risk management maturity with 37 Likert scale questions based on the contents of the standard.

The risk management maturity on average was found to be neither high nor low, thus implying, that the Finnish organizations are lacking behind the requirements of the standard. The results substantiate the intuitive presumption that the large enterprises are more mature in their risk management than the small- and medium-sized companies. The most problematic area were the risk management performance measurement and the quality of communications with employees and external stakeholders.

Table of Contents

ABBREVIATIONS

AS/NZS 4360:2004

Risk Management: AS/NZS 4360:2004

COSO

Committee of Sponsoring Organizations of the Treadway Commission

COSO ERM

Committee of Sponsoring Organizations of the Treadway Commission. 2004. Enterprise Risk Management - Integrated Framework

CRO

Chief Risk Officer

ERM

Enterprise Risk Management

ISO

International Organization for Standardization

RM

Risk management

RMM

Risk maturity model

RMP

Risk management process

1 INTRODUCTION

1.1 Background for the Research

Organizations of all types and sizes face uncertainty regarding their objectives. Uncertainty occurs at every level of an organization and in every operation and function. The effect of this uncertainty on an organization's objectives is "risk" (ISO Guide 73, definition 1.1). In order to ensure the continuance of operations and ultimately, achievement of objectives, organizations need to control the effects of uncertainty. This activity is known as "risk management"[1]. "Risk management" is a concept, which encompasses a plethora of activities in organization. At every level and in every function of an organization, activities to address effects of uncertainty take place.

The emergence of Enterprise Risk Management[2] has been a major recent paradigm change in the field of risk management. The approach emphasizes enterprise-wide management of risk, in which risk management is seen as an integral part of all decision making. Among other drivers, the accelerated pace of globalization has increased uncertainty in many areas of operation. Until the late 1990's, risk management had been mainly practiced in organizational "silos", i.e. as separate functions each with the goals and procedures of their own. However, with the increased complexity caused by the global interconnected economy, it became apparent that the existing tools were not sufficient in dealing with the new operational environment.

To address these needs, a new integrated enterprise-wide approach to risk management evolved. Risk management standards, or "frameworks", are among the most visible contributions to the development of ERM. RM standards have been developed by various professional organizations, national standards bodies and RM practitioners. Their main idea is to present a model for organizational risk management. Typically, these models are generic, which will enable

---

[1] later: *RM*

[2] later: *ERM*

implementation by many different kinds of organizations. There is also a number of industry- or function specific RM standards. However, they will not be examined in the scope of this study, since their nature and scope are fundamentally different from generic RM standards.

In November 2009, the International Organization for Standardization[3] published a new standard for risk management. The new standard is generic, thus applicable to any organization, project, process or even individual. After four years of preparatory work by hundreds of risk management professionals, the completed standard is anticipated to gain a worldwide popularity among risk management professionals (Purdy 2010). The standard was mandated and published by the International Organization for Standardization, which is an international cooperative organ for standards development. Serving as a network of national standard bodies, the Switzerland-based organization is the world's largest publisher of standards. ISO also involves a large number of cooperative organizations with regard to standards development. (www.iso.org 2012b)

Although several studies conclude that there seems to be a widespread agreement on the basic components of a RMP, risk management is still suffering from lack of consensus regarding mutual terminology (e.g. Raz & Hillson 2005; Henriksen & Uhlenfeldt 2006; Ale et al 2010). The attempt of most RM standards has been to create uniformity in risk management practices. However, no standard has so far been able to establish itself as a global best practice solution. Backed by an authoritative publisher, ISO 31000 is the latest attempt to harmonize risk management practices and terminology.

ISO 31000 reflects many aspects typical for ERM, such as integration of RM to organizational processes for a seamless part of daily decision making. The RMP depicted in ISO 31000 is at large the same than in previous standards and identical to the RMP in an earlier standard AS/NZS 4360:2004[4]. ISO 31000 is an attempt to incorporate best practices from preceding risk

[3] later: *ISO*

[4] *Australian/New Zealand Standard: Risk Management: AS/NZS 4360:2004*

management standards, such as COSO ERM[5], AS/NZS 4360:2004 and PMI[6] (Shortreed 2010). The standard adds in a comprehensive vocabulary and an entirely new approach to risk as an *effect of uncertainty*. Moreover, in ISO 31000, risk management is perceived as a trinity of Principles, Framework and Processes, whereas earlier standards have been mainly focused on depicting the process of managing risk. The decision to include the background organizational arrangements supporting the RMP as an equally important component is one of the innovations in ISO 31000.

This study is an attempt to investigate the ISO 31000 -compliance of Finnish organizations. However, ISO 31000 -compliance in itself is merely a proxy for a more important factor, namely the performance of risk management. In other words, the *maturity* of risk management is measured by using the performance criteria set by the standard. The major assumption behind this study is that ISO 31000 represents current best-practice risk management. Using the standard to benchmark risk management performance will provide a valuable insight into quality of risk management currently practiced in Finland.

1.2 Literature Overview & Previous Research

This chapter outlines the literature and research used in this study. ISO 31000 can be perceived as a part of a wider ERM paradigm. Thus, ERM-related literature and research are widely referred to in the context study. Since the publication of ISO 31000 in November 2009, only a few pieces of academic research about the standard have been published so far. The first ones to examine the newly established framework are Purdy (2010), Shortreed (2010), Leitch (2010) and Aven (2011). While Purdy's focus of Shortreed (2010) and Purdy (2010) is on examining different aspects of the new standard in a rather positive tone, Leitch and Aven are excruciatingly critical towards the terminological and functional defects of the new standard. These four studies will be

[5] *Committee of Sponsoring Organizations on Treadway Commission: Enterprise Risk Management - Integrated Framework*

[6] *Project Management Institute: Practice Standard for Project Risk Management*

further examined in chapter 3. In Finnish context, no scientific studies on ISO 31000 have been published yet. Therefore, this present study is the first one to venture into that area.

Hills (2011) has studied ISO 31000's applicability to health emergency management in mass gatherings. For demonstration, the author uses examples from past real-life mass gatherings within Asia-Pacific region and examines them in the ISO 31000 context. However, this piece of research is of little relevance with regard to this present study.

In addition to study publications by professional organizations, such as PwC or Aon, very little academic research on ERM has been conducted so far. A review on ERM-related articles in academic journals and working papers revealed that academic research on ERM is at large descriptive. Moreover, since the research is for most part not motivated by earlier studies, the findings have not been consistent. (Iyer & Rogers & Simkins 2010)

Risk management consultancies and professional organizations have developed risk maturity models to investigate the performance of RM. Models typically include a series of performance criteria, which intend to measure, how well the audited organization is performing in its risk management. Currently used risk management maturity models are examined in chapter 2.4 of this study.

1.3 Research Methodology

The main objective of this study is to find out, how well Finnish organizations are compliant with ISO 31000. The fundamental paradigm for this study is, that an ISO 31000 -compliant *risk management architecture*[7] is a value-adding function in all stakeholders' viewpoint. By examining those areas of operation in which the Finnish organizations are lacking behind the ISO 31000 benchmark, it is possible to enhance the quality of risk management with according corrective measures.

[7] see definition in chapter 1.4

The purpose of this study is to address the following research question:

1. What is the degree of compliance of Finnish organizations with ISO 31000?
    a. In which areas of operation are the organizations lacking behind the performance criteria set by the standard?

Since ISO 31000 is a standard with qualitative requirements, it is difficult to assess whether an organization is totally compliant with the standard. Therefore, ISO 31000 is not certifiable. The key idea of the standard is that by using the presented qualitative elements, each user should tailor the risk management architecture to suit his organization's needs. Despite being slightly impractical considering the nature of the standard, the term "compliance with ISO 31000" is used in this study to refer to the extent of RM maturity measured by the standard.

Compliance with ISO 31000 is an indicator of the *maturity* of risk management. The concept "RM maturity" refers to the performance of an organization's risk management architecture. Some well-known risk maturity models include *RIMS Risk Maturity Model for Enterprise Risk Management*[8] (RIMS 2006), *Aon ERM Risk Maturity Model*[9] by Aon Corporation (Aon 2010) and RM model used by PricewaterhouseCoopers[10] (PwC 2008). In both of these models the maturity of RM is measured by certain attributes, such as board-level commitment to ERM. These models are examined in detail in chapter 2.4.

[8] later: *RIMS RMM*

[9] later: *Aon RMM*

[10] later: *PwC*

The methodological framework for this study is depicted in the Illustration 1 below.

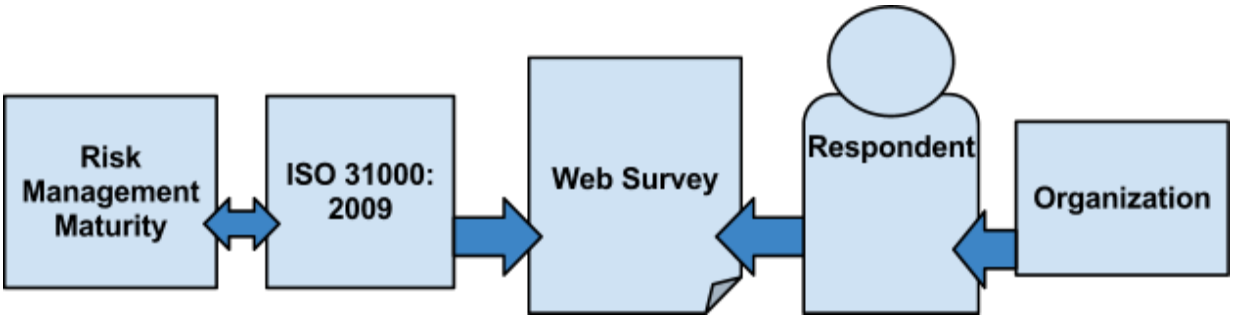


Illustration 1: The research method and according elements

This study attempts to assess the RM maturity of Finnish organizations by using the contents of ISO 31000 as a proxy. Illustration 1 portrays the challenge present in the research setting. The attempt to portray compliance with ISO 31000 (or RM maturity) is made difficult by the three layers of interpretation: the first layer is the survey form, which is an interpretation of ISO 31000. The second layer is between the respondent and the survey, in which the respondent makes his own interpretations about the questions. The third layer is the ability of the respondent to make realistic assumptions regarding the actual state of risk management of his organization. Despite its obvious limitations, survey is a widely used method in ERM research (Iyer & Rogers & Simkins 2010).

Epistemology refers to the philosophical presumptions of a research undertaking, which relate to the issues regarding the essence of knowledge and accumulation of knowledge on the research topic (Jankowicz 2005, 108 - 109). Also the choice of research methods is fundamentally an epistemological issue (Hirsjärvi et al, 126 - 127). A major epistemological presumption with regard to this present study is that the surveyed respondents are capable of sufficiently assessing the state of their background organization. This approach is obviously bold and not entirely without problems. One could argue that reflecting the state of an organization via one person's more or less subjective understanding would produce distorted results. In addition, finding the employee most knowledgeable on the organization may prove to be difficult (Iyer et al 2010). Nevertheless, there are good reasons for the approach taken in this study. One argument for that is that risk manager should by default be the person most aware of issues related to risk

management in the organization. Furthermore, the same assumption has been used in a number of earlier studies (e.g. Schrøder 2006; COSO 2010; Accenture 2011). Other alternative approaches to address the research question are evaluated later in chapter 4.

Operationalization refers to the process of transforming the examined phenomenon into measurable variables. The process of operationalization begins from defining the main concept, which portrays the examined phenomenon of the study. The main concept is defined by different variables, which are intended to define the different qualities of the phenomenon. The variables are further described with *operational definitions*, which are used in the test setting. (Cooper & Schindler 2003, 45 - 46; 428) Operational definitions of the variables are the questions of the survey. The exact composition and questions of the survey are presented in the Appendix 1 of this study.

The *validity* of the operational definitions and research setting in itself is difficult to evaluate, since the performance criteria presented in ISO 31000 are qualitative. Accordingly, the formulation of the survey questions is at large subject to subjective decisions of the author. However, to address this problem, the survey form was pretested with three knowledgeable risk management practitioners before addressing it to the audience.

This present study is mainly *descriptive*, although it includes elements from *reporting* research. "Descriptive" research refers to research, which attempts to present essential, interesting facts regarding certain phenomenon. Correspondingly, "reporting" research ventures into new uncharted areas and phenomena, with the attempt to accumulate data regarding the phenomenon. (Cooper & Schindler 2003, 10 - 11) In some sources, such as Hirsjärvi & Remes & Sajavaara (2007, 134 - 135), an equivalent term "exploratory research" is used to describe elementary-level research of pure data accumulation.

Reports on RM maturity have been published by risk management consultancies such as Aon (2010), Accenture (2011) and professional organizations such as RIMS (2011) and COSO (2010). So far there are no published studies to assess RM performance using ISO 31000 as a framework. This study is the first one to use the standard as a framework for evaluating RM effectiveness.

This study is *cross-sectional*. In other words, it is limited to describing the ISO 31000 -compliance of Finnish organizations at a certain moment of time. A *longtitudinal* study would be suitable for examining the development of ISO 31000 -compliance over time, but it is not possible regarding the scope of this study.

Explanatory research is a form of research, which typically aspires to evaluate causes or consequences for prevailing conditions (Cooper & Schindler 2002, 10 - 11). In this study, causes for risk management maturity are investigated. Consequences are more difficult to evaluate. Based on the results of this study, one can only make vague predictions on future performance derived from the measured risk management maturity. Therefore, due to the limitations of the data, anticipation of consequences is not among the goals of this study.

Earlier studies have focused on measuring the stage of implementation of ERM system, i.e. maturity of risk management. The lack of widely accepted variables regarding the measurement of state of RM has constituted a hindrance for academic ERM research. One commonly used proxy is the appointment of CRO, chief risk officer. This is intended to signal the level of RM awareness in the organization. (Iyer et al 2010) However, this variable is subject to serious limitations, most important of which is the variation of actual role of CRO in the organization.

1.4 Definitions of the Most Important Concepts

For the purpose of clarity and convenience of reading, some concepts that may prove to be a source of possible misconceptions are examined in this chapter. The terminology in the field of risk management is diverse. Alike all social sciences, RM is also subject to reformulation of terminology by different RM practitioners. Even today, there has been a profound lack of consensus regarding some core concepts, such as "*risk*". This creates a huge challenge for anyone who wishes to familiarize herself with theories and practice of RM.

Risk

ISO 31000 defines "risk" as "*effect of uncertainty on objectives*" (ISO Guide 73:2009, definition 1.1). Other existing definitions have more or less different emphases: for instance, some

definitions consider "risk" as inherently adverse, while others recognize the opportunity dimension as well. Different definitions of risk are examined later in chapter 3.3.1.

Risk management

Risk management can be defined as "*coordinated activities to direct and control an organization with regard to risk*" (ISO Guide 73:2009, definition 2.1). ISO 31000 distinguishes between "risk management", which refers to RM architecture, while "managing risk" or "management of risk" refer to applying that architecture on particular risks. In this study, this distinction applies.

Enterprise risk management (ERM)

ERM is a holistic approach to risk management, which emphasizes integration of risk management into all organizational processes and decision making. In addition, ERM highlights taking a strategic perspective on RM. (e.g. COSO 2004, 4) Equivalent concepts to ERM are for instance "*integrated risk management*" (e.g. Miller 1992) and "*enterprise-wide risk management*" (DeLoach 2000; Henriksen & Uhlenfeldt 2006).

Risk management framework[11]

In the field of risk management, the term "*risk management framework*" is used in two senses:

Firstly, *RM framework* refers to a written description of a risk management system (e.g. Shortreed 2010), for instance ISO 31000 or COSO ERM. Some risk management frameworks, such as ISO 31000, refer to themselves to as *"risk management standards*". These two terms are usually used interchangeably in the RM industry (Henriksen & Uhlenfeldt 2006).

Secondly, RM framework can refer to the entity of an organization's risk management system. According to ISO 31000, RM framework is a "*set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization*" (ISO Guide 73:2009,

11 later: *RM framework*

definition 2.1.1). This definition is partially overlapping with the previous one, since a RM standard is fundamentally a depiction of a system of organization's risk management.

ISO 31000 distinguishes "RM framework" from two other parts of an organization's RM system, namely *risk management principles*[12] and *risk management process*. These three components form "*risk management architecture*" (ISO 31000:2009, vi). This division will be examined in chapter 3.3 of this present study.

Since this study relies on ISO 31000 as the most relevant contemporary RM standard, it is the author's intention to use ISO 31000 -compliant terminology whenever possible. Therefore in this study the following definitions apply:

- "*RM architecture"* refers to the entity of an organization's risk management.
- "*RM framework"* refers to the certain component of the RM architecture
- "*RM standard"* and "*RM guide"* refer to a written description of a RM architecture

Risk manager

"Risk manager" refers to the employee responsible for maintaining and developing the RM framework of the organization. In some organizations, risk managers are titled as Chief Risk Officers, but this is not always the case.

Risk management process[13]

RMP is namely a process dedicated to managing risk, namely "*communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring and reviewing risk*" (ISO Guide 73:2009, definition 3.1).

---

12 later: *Principles*

13 later: *RM process*

Risk management maturity

RM maturity refers to the performance of risk management architecture applied in the organization. In the field of RM, equivalent concepts "RM performance" and "RM effectiveness" are also used. In this present study, all of the concepts are used in an equivalent meaning. In the context of this study, ISO 31000 is used as a proxy for measuring the RM maturity. Thus, the expressions "compliance with ISO 31000" or "ISO 31000 -compliance" indirectly refer to RM maturity.

Risk maturity model (RMM)

RMM refers to a model, which is intended to measure the maturity of an organization's risk management.

Risk management industry

In the context of this study, "*RM industry"* refers to the various disciplines of risk management, consisting of practitioners both in the academia and public and business organizations. Also expressions *"field of RM*" and "*RM field*" are used.

Principles (with first letter in MAJUSCULE)

11 Principles for risk management in Clause 3 of Principles & Guidelines.

Attributes (with first letter in MAJUSCULE)

Five Attributes of enhanced RM in Annex A of Principles & Guidelines.

Principles and Guidelines

ISO 31000:2009 - Principles & Guidelines on Implementation

ISO Guide 73:2009

ISO Guide 73:2009 - Risk Management - Vocabulary

2 RISK MANAGEMENT

2.1 What Is Risk?

In everyday language, the word ”risk” is used to describe the danger and uncertainty related to the possibility of an adverse event (e.g. Vaughan & Vaughan 2001, 4). In professional use, the term is used with more diversity, often linked to the specific context of use. However, both individuals and organizations take measures to control uncertainty in order to achieve objectives. These measures are known as “risk management”.

Despite decades of scientific research and discussion, there is no general agreement concerning the exact definition of “risk”. Moreover, the situation is further complicated by the fact that the concept of ”risk” has been been employed by various scientific disciples, such as economics, insurance and engineering sciences. Each one of these disciples uses the concept fitted to the needs of their own theoretical frameworks. (Vaughan & Vaughan 2001, 4) For instance, in the insurance industry, “risk” is understood as a harmful event, which includes no potential “upside”, such as a hail storm or traffic accident. On the contrary, in the area of finance, risks have been traditionally regarded as opportunities, with a chance of both making a profit or losing money. The latter approach from the world of financial risk management has been brought to a wider use with the emergence of ERM. The terminological dispersion is further evidenced in a recent review of RM standards, which reveals that there are great differences in the way that “risk” is defined in different standards (Ale, Aven & Jongejan 2010).

Different definitions of “risk” include for instance (Vaughan & Vaughan 2001, 4):

1. the chance of loss;
2. the possibility of loss;
3. uncertainty;
4. the dispersion of actual from expected results; and
5. the probability of any outcome different from the one expected.

Vaughan & Vaughan (2001, 4) have found two shared elements in the majority of definitions of ”risk”: *indeterminacy* and *loss*. Herein, ”loss” does not simply indicate loss of physical assets or damage, but more broadly, deviation from what is expected or hoped for. “Indeterminacy” with regard to risk is inherently related to future events. In other words, “risk” is not about uncertainty on what has happened previously, but what may happen in the future.

Vaughan & Vaughan (2001,10 - 11) classify risks in two categories: (1) *pure* and (2) *speculative* risks. *Pure* risks are risks with only adverse consequences. Correspondingly, *speculative* risks are risks with both upsides and downsides. In other words, speculative risks relate to decision making and the search for opportunities. Furthermore, pure risks can be divided into *insurable* and *non-insurable* risks.

Risks differ from one another in the sense of importance or noteworthiness. Expressions such as “degree of risk” (e.g. Vaughan & Vaughan 2001) and “level of risk” (e.g. ISO 31000:2009) are used in risk management literature to measure risks with regard to their importance. In a classical measurement of risk, two distinct dimensions are used to evaluate its significance: probability and consequences. “Consequences” refer to the effect of the risk, and correspondingly, “probability” refers to the associated likelihood of the occurrence. (Vaughan & Vaughan 2001, 6 - 7; Suominen 2003, 10). Correspondingly, in ISO 31000 *level of risk* is expressed in terms of the combination of *consequences* (ISO Guide 73:2009, definition 3.6.1.3) and their *likelihood* (ISO Guide 73:2009, definition 3.6.1.1).

Since “probability” is fundamentally a concept used in mathematics and statistics, other words have been employed to describe the degree of uncertainty. For instance, the word “likelihood” is preferred by some risk management practitioners, since mathematical concepts, such as “probability”, inherently indicate that the risk involved is measurable by an exact probability. Also ISO 31000 encourages the use of the concept “likelihood” when determining the uncertainty related to risks. In the context of ISO 31000, “probability” is used to express mathematical probability, as a number between 0 and 1 (ISO Guide 73:2009, definition 3.6.1.4).

Uncertainty is often modeled using statistical data. However, using statistical data to estimate future probabilities has already for a while been subject to debate. The applicability of evaluating

past occurrences to predict the future is problematic, since, among other reasons, the conditions that affected past events are constantly changing. In other words, even if there would be sufficient statistical data to evaluate probabilities with statistical significance, the statistics might not be applicable at all, since the particular phenomenon may not follow the same statistical pattern any longer. (e.g. Bernstein 1996, 6 - 7; 220 - 227)

Risks can be examined in two different dimensions, objective and subjective. Vaughan & Vaughan (2001) semantically differentiate objective ”risk” from ”uncertainty” or ”subjective risk”. Individuals tend to perceive risks differently, based on their subjective evaluation of the conditions and consequences. In some cases, individuals may perceive risks that do not exist at all or on the other hand, fail to detect some risks. This subjective view on risk is distinguished from the objective, actual risk, which exists regardless of the individual’s awareness.(Vaughan & Vaughan 2001, 5 - 6; also see: Kamppinen & Raivola & Jokinen & Karlsson 1995, 17 - 18) Nevertheless, since every risk is fundamentally an affair of unknown future, risk has no objective existence until it has been realized. This is why risk carries the aspect of uncertainty.

An individual's level of expertise regarding the particular risk affects the perception of the particular risk. Experts and laymen have been shown to emphasize different aspects of risk and measure its severity differently. While experts typically emphasize ”hard facts”, such as statistical probabilities or scientific knowledge, non-experts are more likely to assess the risk typically based on emotional factors and shallow knowledge on the topic. (Slovic, 1987)

2.2 What Is Risk Management?

In a computer safety -related risk management guide dating back to 1978, risk management was defined as “*the method of approaching a problem of how to deal with pure threats which threaten an organization...*-” (Pritchard 1978, 2). This definition reflects the approach to risk as an inherently adverse phenomenon. This approach is characteristic for risk management practitioners who perceive risks with regard to insurance or security function (e.g Vaughan & Vaughan 2001, 18 - 19). More recently, the emphasis has shifted from traditional technical-economic loss avoidance to contemporary risk management, in which risk is seen as two-sided, with both upsides and downsides (Henriksen & Uhlenfeldt 2006). In ISO 31000, “risk

management" is defined as "*coordinated activities to direct and control an organization with regard to risk*" (ISO Guide 73:2009, definition 2.1). Risk management is not about avoiding uncertainty, since decision making always involves indeterminacy. The focus on merely avoiding risks means also to ignore the opportunities involved, which will lead to narrowly based decision making (Purdy 2010).

The early 20th century saw the emergence of risk management in its corporate form of application, in which RM served the needs of mitigating the financial consequences of pure risks facing corporations. At this point, risk management was primarily considered as an insurance-buying function. Simultaneously at the society level, the social insurance programs took place to address the new social risks caused by the urbanization and industrialization occurring in the Western Europe and United States. In the mid 1960's, the new managerial philosophies with an emphasis of cost-benefit issues fueled the first major transition in RM. It became obvious, that instead of trying to minimize the costs of transferring risks to a third party, a more thrifty approach was to attempt to minimize the level of risk itself. However, risk management was still typically regarded as management of pure risks (Vaughan & Vaughan 2001, 18).

Risk management failures, such as Barings Bank in 1996, the 9/11 terrorist attack in 2001 and the collapse of Enron in the same year, fueled the second wave of evolution at the break of the third millennium. Additionally, the operational environment in which many of the large corporations worked had become increasingly complex and interdependent. With the increased complexity became the increased uncertainty. New regulation, such as the Sarbanes-Oxley Act in the United States, had been established to address the call for improved corporate governance and visibility, and to control the quality of risk management. (Kloman 2010) In the aftermath of the recent financial crisis in 2008, the importance of risk management is increasing, as corporate managers are increasingly embracing risk management as a high-priority function (Accenture 2011; Branson 2010).

A new RM philosophy titled Enterprise Risk Management was the result of these above-mentioned occurrences. COSO (2004, 4) defines ERM as follows:

"Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

This definition reveals that ERM should encompass all employees, be aligned to the organization's objectives and be included in all decision making. Before the emergence of ERM, risk management had typically been practiced in separate functions inside the organization (Aabo & Fraser & Simkins 2010). An uncoordinated RM could at worst result in a situation where risk controls in one entity would disturb the RM efforts of the rest of the organization. For this reason, ERM emphasizes coordination of RM across the organization.

The fluency of an integrated RM is greatly affected by communications within the organization and with the external stakeholders (ISO 31000:2009, 14 – 15). An important factor herein is the uniformity of the terminology. The field of RM has traditionally suffered from diversity of terminology, which has constituted a major challenge for RM practitioners. RM standards, such as ISO 31000, have attempted to address this problem by providing a proposition for a common terminological framework. However, no RM standard has so far achieved the position as a global agreement on risk management vocabulary.

2.3 Risk Management in Finland

RM -related regulation in Finland can be classified in two categories: mandatory and self-regulative. Mandatory regulation covers Finnish legislation, regulation stemming from the European Union and international financial solidity requirements concerning mainly finance sector. The most significant of self-regulative norms is the corporate governance code for companies listed in local stock exchange.

Besides banking and insurance industries, Finnish legislation sets no requirements regarding business risk management in enterprises. Risk management -related legislation in Finland is limited to consider hazard risks in areas of occupational safety and disaster and fire prevention. Legislation concerning banking sector is currently harmonized with Basel II accord. Correspondingly, insurance industry is subject to special legislation with basis on Solvency

directive by European Commission (73/239/EEC). Solvency directive and Basel accord are both currently being revised to answer the need for improved risk management in financial institutions (Al-Darwish, Hafeman, Impavido, Kemp & O'Malley 2011). Solvency of financial institutions is seen as a key issue for the functionality of society, whereas other businesses are allowed to freely pursue their desired aggregate level of risk with a possibility of bankruptcy.

Public companies listed in Nasdaq OMX Helsinki stock exchange are subject to a special corporate governance code by Finnish Securities Market Association[14]. The association is a cooperative organ, whose purpose is to maintain and develop the corporate governance in Finnish public companies. The association has no official or legislative enforcement power over the public companies. However, the self-regulative recommendations and codes issued by the association are widely followed by public companies.

The corporate governance code for public listed companies requires that enterprises should explicate their known major risk exposures and the principles, according which the RM is arranged. The code encourages presenting a statement of contemporary major risks and uncertainty factors in annual and quarterly reports. (Arvopaperimarkkinayhdistys 2010) Risk management -related self-regulative guidance can also be found in a recommendation for unlisted companies by Finnish Central Chamber of Commerce (CCC 2006).

2.4 Risk Management Maturity

The term "RM maturity" is used to refer to the level or performance of the RM architecture. "Maturity" is a quality that is achieved organically, in other words being "ripe" or "fully developed" (Hillson 2010, 50). However, in the case of "risk management maturity", it is likely that a "mature" risk management architecture is before all a result of conscious efforts rather than chance or the natural evolution of things. In the risk management literature, "ERM" is sometimes used as a synonym for a fully mature RM, as a fulfillment of an implementation project (e.g. Aabo et al 2010). The word "implementation" is used to describe the pursuit for the aspired state

[14] in Finnish: *Arvopaperimarkkinayhdistys*

of risk management that is built upon the principles of ERM. Semantically, “implementation” refers to conscious adaptation of certain elements (see e.g. Longman 2003, 814).

However, in RM literature, there is no mutual agreement on what constitutes a fully “mature” or “implemented” risk management. In addition, as ISO 31000 highlights, the RM framework needs to be continually upgraded to correspond the changes in internal and external contexts (ISO 31000:2009, 13). Therefore it is questionable whether RM can be regarded as having achieved full maturity, since it is in a constant state of adaptation like the rest of the organization (Hillson 2010, 50 - 51).

Risk maturity models are typically qualitative models, which aim at describing the current stage of implementation of ERM in an organization. Risk maturity models typically consist of attributes, which are intended to describe essential characteristics for ERM, such as board commitment to RM. Different stages of maturity are assigned to the attributes to describe the level of progress. All of the three RMMs presented in this study use a five-stage scale to evaluate the maturity of the particular area. Illustration 2 summarizes the attributes used in three risk maturity models and ISO 31000:2009.

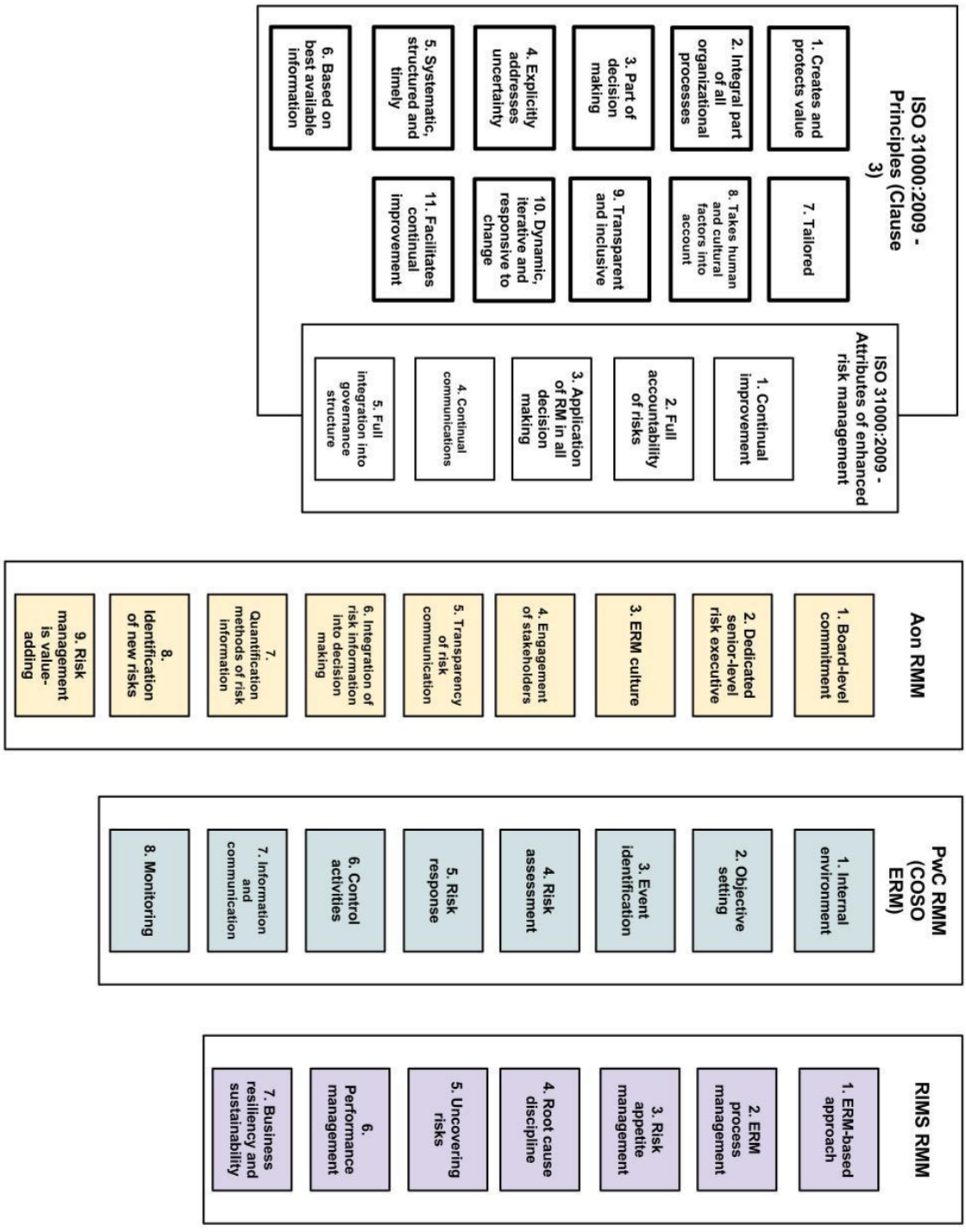


Illustration 2: Elements of different risk management maturity models

The comparison of different risk maturity models is challenging due to the heterogeneous composition and terminology. Each of the models has a different perception on what the necessary elements of RM are. To assess RM maturity, ISO 31000 offers a set of RM performance criteria, the *Principles* and the *Attributes* (Shortreed 2010), which are partly overlapping. Whereas Aon's (2010) RMM includes nine "hallmarks", or attributes, PwC's (2008) has eight and RIMS's (2006) seven. Since the attributes presented are not usable *per se* without further clarification about what is measured, the text bodies of the RMMs provide expand the ideas behind the attributes. RIMS provides a list of key drivers, that is, the operationalization of the attributes. Such ready operationalization is not presented in the other three RMMs.

PwC (2008) has adopted its RMM from COSO ERM's (2004) components, which corresponds to the Risk Management Process in ISO 31000 and similar components present also in majority of other RM standards (Henriksen & Uhlenfeldt 2006). Compared to other notable RMMs, the model of PwC is the most narrowly defined, since it at large ignores the RM framework, i.e. the foundations and organizational arrangements to support the management of risk.

In all of the maturity models, alignment of RM objectives to organizational objectives is at some level present. Additionally, monitoring and improvement of the framework were also included in all of the models. As the study of Henriksen & Uhlenfeldt (2006) implies, continual improvement of RM has been widely incorporated in RM practices. PwC's RMM was the only one not to include managers' support to ERM.

RMMs by RIMS (2006) and PwC (2008) are most visibly lacking of stakeholder-orientation present in ISO 31000 and Aon RMM. ISO 31000 encourages to take into account the stakeholders' perceptions and opinions and communicate with them on a frequent basis. However, the lack of stakeholder-orientation in RIMS and PwC[15] may partly be explained by the advances in RM thinking, which has taken major leaps in the wake of the latest financial crisis of 2008.

Aon (2010) sees appointment of a dedicated senior-level risk executive as an indicator of a mature RM architecture. ISO 31000 more vague regarding this topic, indicating management and

[15] *RMM* based on COSO (2004) ERM

board commitment, but makes no remark of the need of a dedicated risk management executive. The appointment of a Chief Risk Officer has been used as an indicator of ERM implementation, i.e. high RM maturity (see e.g.: Liebenberg & Hoyt 2003; Pagach & Warr 2011) Consequently, Beasley, Clune & Hermanson (2005) found that the presence of a CRO in the organization correlated with the perceived RM maturity.

Aon emphasizes quantification of risk information, whereas ISO 31000 takes a more tailored approach by encouraging risk information, whether quantitative or qualitative, to be suited to the need of the particular context. Other maturity models do not address this issue. Both RIMS and ISO 31000 (ISO 31000:2009, 17) consider root cause analysis as an important part of risk management. Risks and their causes and sources should be investigated to gain an articulate understanding of the particular risk. However, unlike ISO 31000, RIMS does not consider interconnectedness of different risks.

Surprisingly, research reports using the existing RM maturity models are few in numbers. In the study of RIMS (2011), the RM maturity was found to be at a satisfactory level. On the contrary, surveys by COSO (2010) and Aon (2010) indicate overall low RM maturity. However, no unambiguous conclusions can be drawn from the results of these three investigations. In addition to using an entirely different scale, they were targeted to geographically and professionally different respondents.

2.5 Roles in Risk Management

This chapter introduces the different roles in risk management with regard to the organization's employees. The concept "risk manager" is used to describe the employee who has the main responsibility to maintain and develop the RM architecture in the organization. Other facilitators include the board of directors, senior management, and internal and external auditors (Branson 2010). These actors will participate in the improvement of RM architecture each with their own contribution.

ERM emphasizes that the responsibility for managing risks belongs to all decision-makers, who need to be held accountable for the risks facing their own area of operation. Therefore, rather than managing risks, the risk manager's role is to facilitate the management of risk. (Shortreed

2010; ISO 31000:2009, 7) Furthermore, due to the sheer diversity of risks, it is nearly impossible to account a single risk manager to manage all the risks of the organization. (Vaughan & Vaughan 2001, 27 - 28).

The scope of the risk manager's duties varies between organizations. The size and industry of the organization affect whether an organization has a risk manager on a full-time basis, or whether the responsibility for the development of risk management is a part-time duty. Large corporations tend to have more resources for the RM function when compared to smaller organizations, wherein the risk manager typically has other duties to employ him (Suominen 2003, 28). The risk manager's role usually depends on the history and development of the RM function in the particular organization. Many risk managers have their background in insurance, security or finance (Vaughan & Vaughan 2001, 26).

At present, risk management in organizations is a diverse field with several actors. Typical actors in the scene of RM are presented in the Illustration 3 below. However, the model presented is most typically applied in the context of large corporations with sufficient resources to maintain a comprehensive risk management framework. Smaller organizations tend to have a more streamlined approach to risk management.

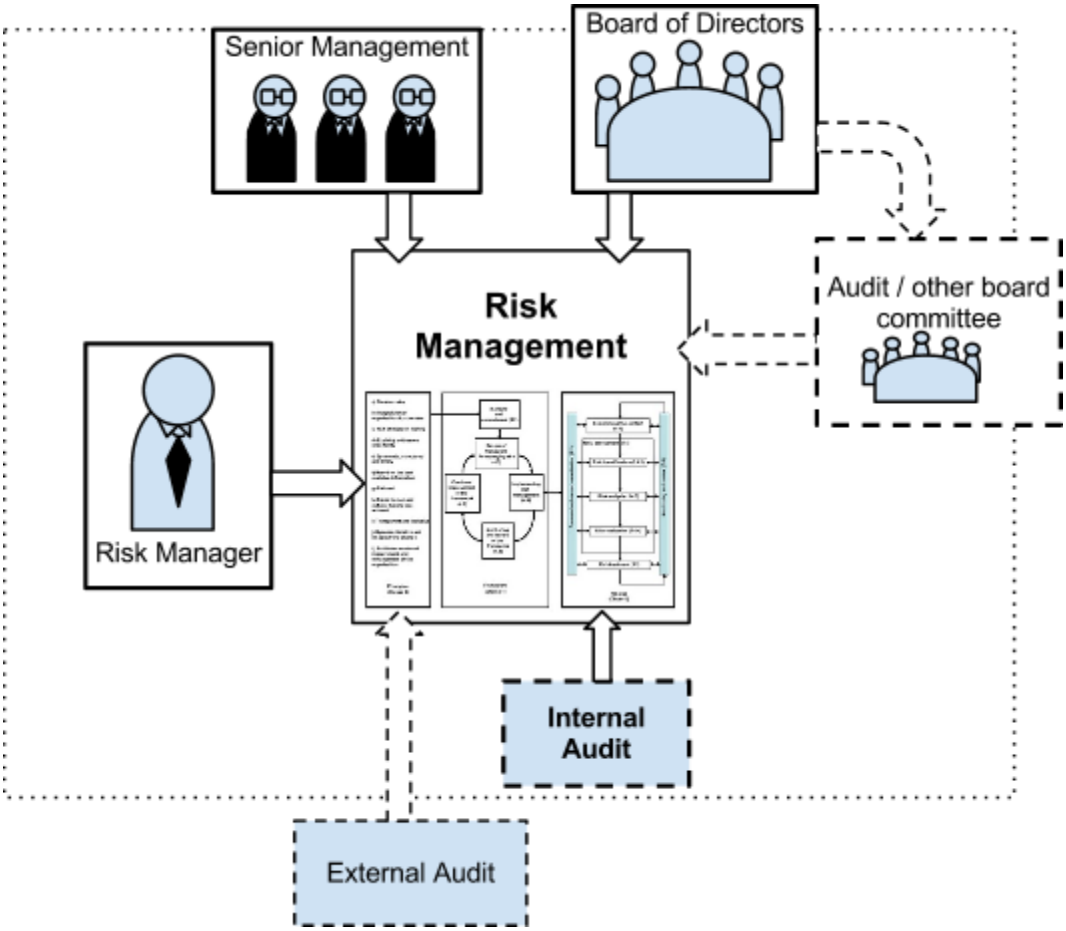


Illustration 3: Roles in risk management (Branson 2010)

The role of the senior management and the board of directors is to give their mandate and commitment to the ERM implementation. Within ERM implementation, senior management's main role is to provide their visible leadership for the project. As representatives of the owners, board members need to communicate the value-adding quality of ERM to shareholders. Typically, the board also has an oversight on RM. Major risks need to be brought to the board's attention. In some cases, the RM supervision can be delegated to a specialized RM committee. Internal and external audit functions evaluate the RM processes, governance and compliance with RM policies. (Branson 2010)

The idea of a specialized risk management executive evolved in the 1950's. Back then, risk managers were more or less perceived as insurance professionals. It was not until the beginning

of the 2000's when companies began appointing dedicated risk managers, Chief Risk Officers[16], with an integrated and truly enterprise-wide oversight on risk management. With the increasing importance of RM, the internal and external audit practitioners would expand the traditional scope of their profession into risk management compliance issues. (Mikes 2010; Kamiya & Shi & Schmit & Rosenberg 2007)

Mikes (2010) classifies CRO roles into two broad categories, namely (1) controller and (2) strategic advisor. The (1) controller role of the CRO emphasizes quantitative risk models and measuring aggregate risk profiles, whereas the (2) strategic advisor is geared towards utilizing qualitative judgement and intimate knowledge of the organization's processes. The approach to whether risks should be modelled quantitatively or qualitatively is the dividing line in most cases between these two broad classifications. (Mikes 2010; also see: Bernstein 1996, 334 - 337)

In their case study, Aabo et al (2010) present an example of ERM implementation. The study implies that the main task of CRO is to manage the implementation of ERM, which is typically a project of several years. As RM maturity is achieved, the CRO's work load is significantly reduced, since the RM architecture is already embedded in all decision making and organizational processes. In theory, a fully implemented ERM is such that no CRO is needed. This situation is evidently highly theoretical. Nevertheless, in the case of the example organization, due to the new well-functioning ERM system, the CRO needed to dedicate a mere 20% of his time to RM-related tasks. The CRO's new role with regard to RM was to maintain and develop the RM architecture and participate in various projects, where RM-related expertise was needed. (Aabo et al 2010)

2.6 Risk Management Standards

The evolution in the RM field is characterized by publication of various RM standards, which attempt to give guidance with regard to practicing management of risk in organizations. Since the publication of the first risk-related standard in 1991, RM standards have achieved a central role in

[16] later: *CRO*

shaping the field of RM. Although the first RM standard was of Norwegian origin, Anglo-American countries have been forerunners in developing risk management standards. (Henriksen & Uhlenfeldt 2006) One of the first generic RM standards was AS/NZS 4360:1995, which brought together for the first time several of the different subdisciplines of RM (Kloman 2010).

Risk management standards can be divided into two broad categories, namely *generic* standards and *industry-* or *function-specific* standards. Generic standards focus on describing an organizational framework for all risk management processes. Typically, they are qualitative by nature, and applicable to a wide range of organizations with different sizes and industries. On contrary, specific RM standards usually focus on a single function, for instance in terms of technical devices or organizations in certain field of business, such as finance. Certification by an external evaluator is widely used with regard to standards to verify their use in the organization. However, the lack of precise requirements makes it difficult to provide certifications to generic RM standards (Raz & Hillson 2005). This study focuses on the rather homogeneous group of generic RM standards, ISO 31000 among them.

A recent research report by COSO reveals that COSO ERM is the most widely used RM standard among the surveyed RM practitioners. The survey indicated that more than a half of all respondents used COSO ERM as a principal standard for RM. Correspondingly, merely 1,9% used ISO 31000 and 1% AS/NZS 4360:2004. (COSO 2010) However, since this research was conducted via COSO member organizations, which operate in the field of accounting, finance and internal audit, it is likely that the results are somewhat biased towards COSO's own RM standard COSO ERM. This assumption is supported by another survey by RIMS (2011), which indicated that COSO ERM and ISO 31000 were almost equally popular among surveyed organizations.

The joint standard AS/NZS 4360:2009 by the standardization organizations of Australia and New Zealand was considered as one of the most widely used worldwide risk management standards. ISO 31000 has largely adopted the same risk management process as described in AS/NZS. Furthermore, both the standards emphasize integration of risk management into organizational processes and practices. (Purdy 2010)

RM standards have been compared in several scientific studies from various perspectives (see: Raz & Hillson 2005; Henriksen & Uhlenfeldt 2006; Ale, Aven & Jongejan 2010). Raz & Hillson (2005) compared nine major RM standards, discussing their differences, similarities and overall applicability. Henriksen & Uhlenfeldt (2006) evaluated four RM standards and their approach to risks arising from strategy process. Ale et al (2010) examined ten RM standards with regard to the definition of basic concepts, such as "risk".

AS/NZS 4360 was the only standard included in all the studies. In addition, two of the studies examined COSO ERM (2004) and IRM/AIRMIC/ALARM (2002), which is *de facto* the same as FERMA's (2003) RM standard. In all of the studies, striking similarities were found in the way that the process for management of risk was defined. The set of standards analyzed by Raz & Hillson (2005) differed from each other by (1) role of additional elements to the RMP and (2) the defined organizational structure supporting RMP.

Ale et al (2010) have found that RM standards suffer from overall ambiguity in terms of terminology. They argue that many key concepts used in the standards are left undefined and thus open for interpretation. Thus, this would indicate that some RM standards are not able to create a meaningful and consistent RM terminology.

Among other concepts, "risk" has been defined in a multitude of ways (Raz & Hillson 2005; Ale et al 2010). In Raz & Hillson study, the definitions of "risk" were classified as "negative", "neutral" and "broad". Negative definitions represented the traditional, insurance-based view on risk. Neutral definitions, such as of AS/NZS 4360:2004, avoid defining risk as negative or positive. Broad definitions consider both the upside and the downside of the risk. An example of a broad definition can be found in IRM / AIRMIC / ALARM Risk Management Standard[17] (IRM / AIRMIC / ALARM 2002).

To illustrate the differences between "neutral" and "broad" definitions of risk, an example of both is presented. In AS/NZS 4360 "risk" is defined as "*the chance of something happening that will have an impact upon objectives*" (AS/NZS 4360:2009, definition 1.3.13). This definition does not

[17] later: *IRM*

take a direct stance on whether risk is adverse or desirable. Correspondingly, IRM formulates "risk" with a sightly different emphasis: "*Risk can be defined as the combination of the probability of an event and its consequences --- In all types of undertaking, there is the potential for events and consequences that constitute opportunities for benefit (upside) or threats to success (downside)*"(IRM 2002)

The difference between "neutral" and "broad" definitions is only minor, since "neutral" definitions inherently assume that risk includes consequences or impact, any of which must be either negative and/or positive regarding the organization's objectives. One possible interpretation is, that the intention of "neutral" definitions is to highlight the multifaced nature of risk as source of both good and bad effects, being inherently neither.

Regarding the above-mentioned essential differences in risk management standards, Raz & Hillson (2005) conclude that there be a need for a new, comprehensive RM standard to amend the problems found in the existing standards. At the time of publication of the Raz & Hillson study, there were only vague rumors and plans of the new upcoming RM standard by ISO 31000. The authors didn't place messianic expectations of the possible future standard, but on the contrary, were doubtful about the abilities of ISO to constitute a best-practice RM standard, which would rectify the problems Raz & Hillson had encountered in the existing standards.

Henriksen & Uhlenfeldt (2006) evaluated RM standards with regard to their focus on strategy process and in particular strategy formulation. They argue that recent RM standards are not successful in creating focus on managing strategic risks, although they claim to do so. The standards also fail in giving advice on "risk consolidation". "Risk consolidation" refers to the process where key risks are prioritised, selected and communicated to the organizational decision makers. The standards examined by Henriksen & Uhlenfeldt (2006) were COSO ERM (COSO 2004), AS/NZS 4360:2004, DeLoach EWRM (DeLoach 2010) and FERMA (2003).

Despite the differences in wording and terminology, the structures for the process of managing risk were nearly identical (Henriksen & Uhlenfeldt 2006; Raz & Hillson 2005). Below in Illustration 4 (Henriksen & Uhlenfeldt 2006) is presented a generic RMP, which presents the structure of the four above-mentioned frameworks. All of the frameworks share structural

similarities with regard to different stages and continuous feedback and information about the management of risk.

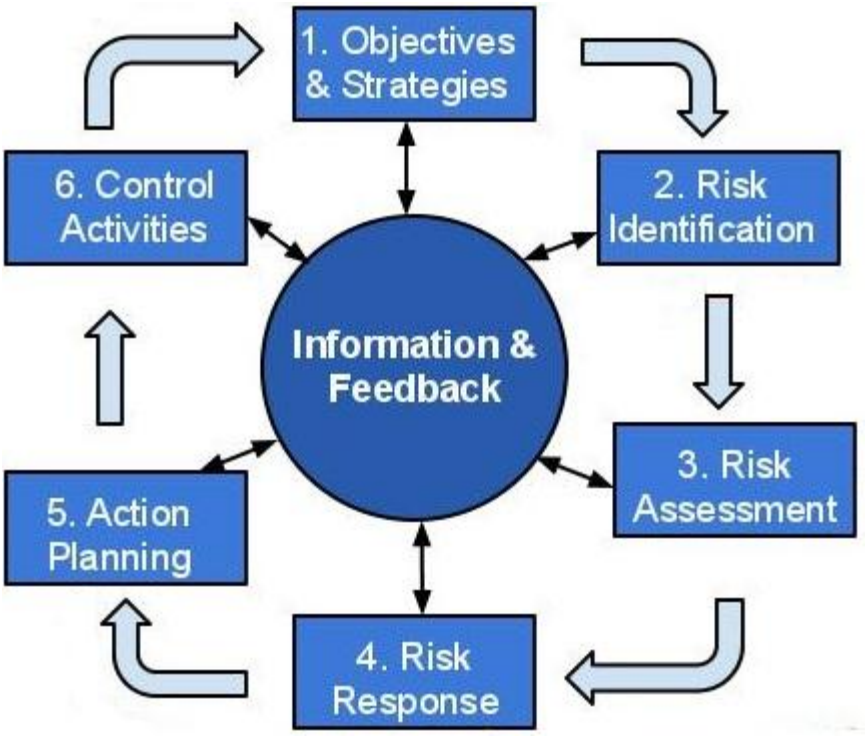


Illustration 4: The generic risk management process (Henriksen & Uhlenfeldt 2006)

Management of risk can be depicted as a continuous six-step process. Risk management is defined by organization's objectives and strategies (1.), which will affect risk management objectives. In all of the four frameworks, risk identification (2.) is performed with regard to event identification. During this stage, events with potential impact on objectives of an organization are identified. Risk assessment (3.) considers the level of risk. Risk response (4.) and action planning (5.) phases include the responsive measures to control and monitor the risk. Based on the level of risk, the particular risk is reacted upon by e.g. sharing the risk or retaining it. Consequently, according action plans and accountabilities are defined. Finally, the efficiency of risk response measures is controlled and new actions decided upon, when needed (6.). Information and feedback are present in every stage of RMP, such as in ISO 31000.

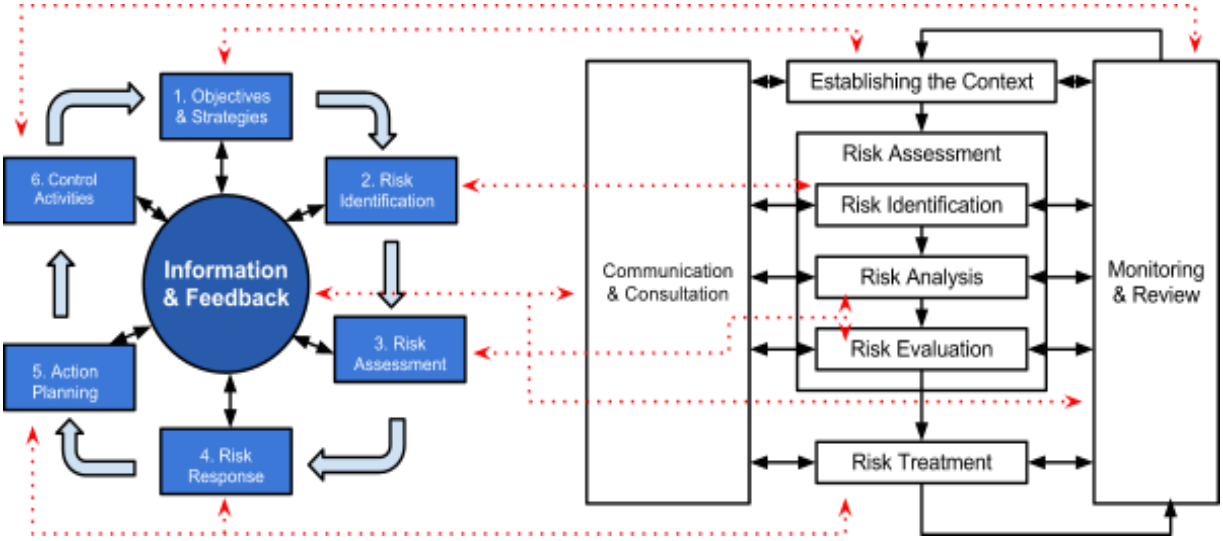


Illustration 5: Comparison between the generic risk management model (Henrikson & Uhlenfeldt 2006) and the

Despite the terminological differences, the RMP presents striking similarities to the corresponding process in ISO 31000. Corresponding stages in Henriksen & Uhlenfeldt -model and ISO 31000 are indicated in Illustration 5 as follows:

- (1.) corresponds “establishing the context”
- (2.) corresponds “risk identification”
- (3.) corresponds “risk analysis” and “risk evaluation”
- (4.) and (5.) include elements similar to “risk treatment”
- (6.) and “Information and feedback” include elements simialr to “monitoring & review”
- “Information & feedback” corresponds “communication & consultation”

Comparison of the synthesis RMP (Henriksen & Uhlenfeldt 2006) with the RMP of ISO 31000 reveals that the RMP somewhat similar to those in the preceding standards. Although the Henriksen & Uhlenfeldt’s study covers only four of all existing RM standards and guides, three of the four standards examined, COSO ERM, AS/NZS and FERMA, are estimated to be the three most influential RM standards worldwide (RIMS 2011). Thus, it can be concluded that when it

comes to the structure of the RMP, ISO 31000 has at large established itself in the same intellectual continuum as the preceding standards.

3 ISO 31000

This chapter presents the main contents of ISO 31000:2009. Firstly, the background and objectives of the standard are evaluated, with according overview on the roots of the standard. Subsequently, in chapter 3.3 on the contents of Principles and Guidelines, the core of the family of ISO 31000 -documents, are examined. This includes the composition of the RM architecture, namely the Principles, the RM framework and the RM process. Being an essential element of standards and risk management, terminological decisions in ISO 31000 are assessed in chapter 3.3.1. The section 3.4 is dedicated to an overview of academic criticism on ISO 31000. TO preserve the original tone of standard, this chapter utilizes as much as possible the original terminological choices used in the document.

3.1 Background

ISO 31000 is an international standard for risk management by International Organization for Standardization[18]. The purpose of ISO 31000 is to offer generic guidelines of establishing a risk management framework, in context of which management of risk is applied. The standard is intended to be applicable for organizations of every size, industry and type.

Currently the standard includes three distinct risk management -related volumes, which are:

- ISO 31000:2009 - Principles and Guidelines on Implementation
- ISO Guide 73:2009 - Risk Management - Vocabulary
- ISO/IEC 31010:2009 - Risk Management - Risk Assessment Techniques

In this study, we focus on the first volume, which is *ISO 31000:2009 - Principles and Guidelines on Implementation*[19]. *Principles and Guidelines* is the heart of the ISO 31000 family, the other two members being mainly auxiliary. *Principles and Guidelines* includes a description of the risk

[18] *ISO*

[19] later: *Principles and Guidelines*

management Principles, framework for managing risk and RM process. For the purpose of clarity, the triad of Principles, RM framework and RM process is defined as the "RM architecture" to distinguish it from the expression "RM framework".

"RM framework" is used in ISO 31000 solely to refer the specific part of *Principles and Guidelines* (ISO 31000:2009, vi). However, in the RM literature, the concept "RM framework" is typically used to refer to a RM standard. (e.g. Ale, Aven & Jongejan 2010; COSO 2004). The frameworks portrayed by the earlier RM standards have focused mainly on the RMP-part of the risk management, ignoring the supporting framework.

ISO/IEC 31010:2009 - Risk Management - Risk Assessment Techniques[20] includes risk assessment application techniques based on the implementation of RM approach introduced in *Principles and Guidelines*. As later described, risk assessment is a part of RM process described in *Principles and Guidelines* and thus it shall be examined in more length and depth in the according chapter 3.3. *Risk Assessment Techniques* is intended to support the implementation of ISO 31000 (*Risk Assessment Techniques*, 7). It includes some established risk assessment methods, such as scenario analysis and HAZOP. Thus, it does not present any significant theoretical contribution regarding risk management. The methods presented in Risk Assessment Techniques are not examined in the scope of this study, since they are not specific to ISO 31000, but rather introduced as a general guidance to assist risk professionals (www.iso.org 2012c).

ISO Guide 73:2009 - Risk Management - Vocabulary[21] is a vocabulary standard for risk management, including definitions for a number of essential risk management terms. A majority of these terms are also listed in Clause 2 of *Principles and Guidelines*. ISO Guide 73:2009 is intended to replace an earlier RM vocabulary ISO/IEC Guide 73:2002, published in 2002. With the introduction of ISO 31000, the earlier vocabulary from 2002 was revised to correspond the new approach to risk, namely the transition from earlier "safety aspects of risk" to the new, neutral stance present in ISO 31000. (ISO Guide 73:2009, v-vii)

---

20 later: *Risk Assessment Techniques*

21 later: *ISO Guide 73:2009*

ISO 31000 was composed by a specialized technical committee formed by ISO. The committee consisted of representatives of ISO member bodies and other risk management experts from specialized organizations (e.g. Purdy 2010). ISO 31000 is considered to synthesize best RM practices from various preceding standards, such as AS/NZS 4360: 2004 and COSO ERM (Shortreed 2010). AS/NZS, a mutual effort by standards organizations of Australia and New Zealand, has in particular influenced the risk management ideals behind ISO 31000.

While ISO 31000 has gained popularity in Australia, it has not yet been widely adopted in US or UK (Everett 2011). However, no academic research has been conducted to validate the popularity of ISO 31000. Surveys by RIMS (2011) and COSO (2010) show mixed results in terms of how widely ISO 31000 has been embraced by RM practitioners. This deficiency of information is partially answered by this study, which, in addition to mapping ISO 31000 compliance, will also simultaneously investigate, how widely ISO 31000 has intentionally been adopted by Finnish organizations.

In the autumn 2011, a global survey was initiated by a LinkedIn group dedicated to ISO 31000. The intention of the survey was to examine, how widely ISO 31000 had been implemented by organizations and how well the respondents were aware of its main principles. The survey ran from 17 October to 30 November. The results of this survey are reflected in chapter 5. (www.iso.org 2012b)

A new project committee by ISO was established in 2011 to prepare a new document for the ISO 31000 family, a guide for the implementation of ISO 31000. The work name for the new standard is *ISO 31004 : Risk management -- Guidance for the implementation of ISO 31000.* The project is currently on a preparatory state and is expected to continue for a yet undefined amount of time. (www.iso.org 2011d)

3.2 Objectives of ISO 31000

ISO 31000 is fundamentally a generic guide to risk management. The work group behind ISO 31000 has ambitiously defined the standard as applicable to *"any type of risk, whatever its nature, whether having positive or negative consequences"* and for *"any public, private or community enterprise, association, group or individual."* In addition, risk management is

ubiquitous, applicable *"throughout the life of an organization"* and to a *"wide range of activities, including strategies and decisions, operations, processes, functions, projects, products, services and assets."* (ISO 31000:2009, 1)

Being an ambitious effort to manage "all risk everywhere", the standard does not attempt to guide risk management with detailed and quantitative specifics, but rather to depict an ideal risk management system with certain iterative processes (Leitch 2010). Iteration is present in continual monitoring and improvement of RM framework. In order to attain simplicity and convenience of application, ISO 31000 was created as a "principal-based" RM framework. In other words, the qualifications of RM architecture set by ISO 31000 are intentionally broad, so that the standard can be applied in any context. (Shortreed 2010)

ISO 31000 is, in addition to its main function as a tool for enterprise risk management, also applicable as the basis for other more specialized standards, constituting a "paramount standard" (ISO 31000:2009, 1). Herein, mutual basis is beneficial especially in terms of vocabulary and terminology. ISO has already begun the work to harmonize its previously published standards with ISO 31000. The creation of ISO 31000 has been strongly motivated by the fact, that the RM industry has traditionally suffered from the diversity of risk management -related terminology, which predictably causes challenges with communicating risk information. One of the goals of ISO 31000, in addition to providing a sound, contemporary RM architecture applicable to any organization, is to harmonize the language used in the RM industry and academia. (Purdy 2010)

Unlike many other ISO standards, ISO 31000 is not intended for the purpose of certification (ISO 31000:2009, 1). Shortreed (2010) considers this as a result of RM architecture being fully integrated in the existing management structure, as stated in ISO 31000. Since there is no uniform way of implementing ISO 31000, certification would be a sheer impossibility.

3.3 Contents of Principles and Guidelines

Principles and Guidelines consists of five Clauses. In the first Clause, the scope and objectives of the standard are briefly defined. Clause 2 defines risk management terminology, sourced from another member of ISO 31000 family, *ISO Guide 73:2009*. In Clause 3, Principles for effective RM are defined. Clause 4 describes a model for arranging RM framework and process of

managing risk is presented in Clause 5. In Annex A, typical attributes of a mature RM are described.

3.3.1 Terminology

Terminology is one of the dimensions of ISO 31000, which are anticipated to greatly influence the risk management industry and science (Leitch 2010). However, the terminology of the new standard has been subject to some criticism from the risk management academia (e.g. Aven 2011; Leitch 2010). Main reasons for the emergence of critical voices has been the vagueness of certain key terms in ISO 31000. The criticism is reviewed in greater detail in chapter 3.4.

In ISO 31000 "risk" is defined as "*effect of uncertainty on objectives*" (ISO Guide 73:2009, definition 1.1). Furthermore, in Note 1 of the definition 1.1, "effect" is explicated as "*deviation from the expected - positive and/or negative*". ISO 31000 has embraced a neutral approach towards defining risk (Purdy 2010), instead of expressing risk in the conventional way as an event with undesirable consequences. Purdy (2010) notes that "*...it is now widely understood that risk is simply a fact of life and is neither inherently good nor inherently bad. To avoid it entirely is to forgo the opportunity of pursuing objectives.*"

In the Raz & Hillson (2005) classification, "neutral" definitions of risk emphasize taking no stance on defining risk either negatively or positively. However, as concluded earlier in this study, the difference between a "neutral" or "broad" definition is only slight. This definition of risk is not entirely new, since the same idea of neutrality of risk has been incorporated in the doctrinal predecessor of ISO 31000, namely AS/NZS 4360:2004. Herein "risk" is defined as (AS/NZS 4360: 2004, definition 1.3.13) "*...the chance of something happening that will have an impact on objectives."*

Risk management is defined in ISO 31000 as "*coordinated activities to direct and control an organization with regard to risk*" (ISO Guide 73:2009, definition 2.1). Although ISO 31000 does not use the concept "ERM", it is fundamentally part of the same paradigm (Shortreed 2010). COSO ERM defines risk management as identification of events that may have an impact on the organization. "Risk" is an *event* with a negative impact, whereas "opportunity" is an event with a positive outcome. (COSO 2004, 21)

As opposed to "event-based" definitions of risk, such as COSO ERM, in ISO 31000, risk management is understood as effects, which can originate from sudden occurrences or long-term changes. By defining "risk" as "effect-based" as opposed to "event-based", the focus can be shifted from analyzing events to analyzing effects. This paradigm shift will reveal more clearly that risk management is about optimizing decision making in order to make achieving objectives more likely. (Purdy 2010)

The terminological choices are an important part of creating a shared understanding on the essence of risk management in organization. This, in turn, is a prerequisite for the integration of risk management as a part of everyday management and decision making. One of the most fundamental shifts in the contemporary risk management has been the expansion of the concept "risk" to encompass both negative and positive outcomes. However, since risk management has traditionally been a playing field of many different disciplines, finding a mutual understanding on key terms may prove to be challenging. Especially the insurance industry has been a major influence for understanding risk management as management of adverse events. (e.g. Kloman 2008, 67 – 75)

3.3.2 Principles

A set of performance criteria is provided to establish a benchmark for effective risk management. The RM performance criteria are presented in the 11 Principles in Clause 3 and five attributes of "enhanced risk management" presented in Annex A (Purdy 2010). The key outcome of successful RM are (1) current, comprehensive understanding of risks, and (2) risks being within the defined risk criteria (ISO 31000:2009, 22).

The 11 Principles are defined as follows (ISO 31000:2009, 7):

1. RM creates and protects value;
2. RM is an integral part of all organizational processes;
3. RM is part of decision making;
4. RM explicitly addresses uncertainty;
5. RM is systematic, structured and timely;

6. RM is based on the best available information;
7. RM is tailored;
8. RM takes human and cultural factors into account;
9. RM is transparent and inclusive;
10. RM dynamic, iterative and responsive to change; and
11. RM facilitates continual improvement of the organization.

In addition, to the Principles, which are intended to describe the basic characteristics of ERM, the appendix of ISO 31000 includes attributes of RM excellence. The excellence characteristics are (ISO 31000:2009, 22 - 23)

- continuous improvement in the framework;
- full accountability for risks;
- application of the RMP in all decision making with appropriate documentation;
- constant communications about risk management; and
- full integration in the organization's governance structure.

Shortreed (2010) infers that the Principles are intended to describe the basic attributes of an effective RM. Correspondingly, the characteristics of excellence can be found in the attributes of Annex A. (also see: Purdy 2010) However, the two sets of performance indicators are thematically very similar, emphasizing the same issues.

The RM architecture (see Illustration 6) is depicted in the standard with a single large diagram (ISO 31000:2009, vii), which includes the principles for managing risk and two processes: one for the continuous improvement of the framework for managing risk and other for managing risk, i.e. RMP. The framework is defined in Clause 4 and RMP in Clause 5 of the standard. The content of these clauses is examined in following chapters 3.3.3 and 3.3.4.

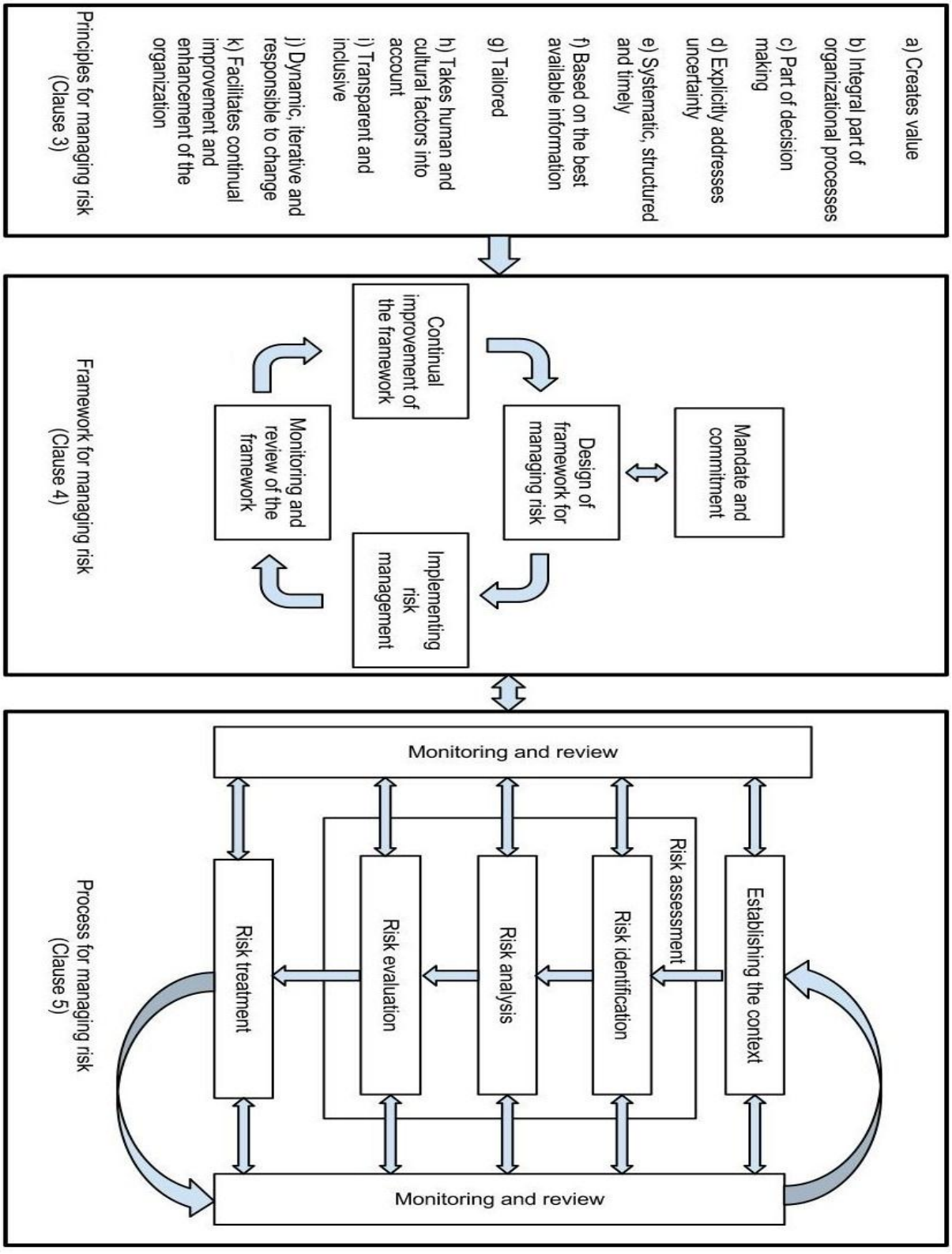


Illustration 6: The risk management architecture

Illustration 6 is adapted from the corresponding portrayal in *Principles and Guidelines*. ISO 31000 defines this depiction as "*relationships between the risk management principles, framework and process*." (ISO 31000:2009, vii) Management of risk occurs in the setting of RM framework, which consists of according *foundations* and *organizational arrangements* to facilitate the management of risks throughout the organization (ISO 31000:2009, 8; ISO Guide 73:2009, definition 2.1.1). A large organization may have hundreds or thousands of RMPs, each representing an individual risk, with varying depth and importance (Shortreed 2010).

As Leitch (2010) remarks, no explanation is provided to clarify the meaning of boxes and arrows. On the other hand, this criticism seems slightly contrived considering the fact, that the diagram is somewhat logical and compliant with the contents of the standard. The diagram depicts the RM architecture, foundation of which are the overarching principles. The RM framework and RM process are interrelated in order to produce the output of RM, which, in case of successful implementation, is achievement of organization's objectives.

3.3.3 Risk Management Framework

The framework for managing risk (Illustration 7) is an iterative process of designing, implementing, monitoring and reviewing and continually improving the risk management. It is facilitated by *mandate and commitment* of the *management of organization*. In addition to commitment of the management, commitment of the whole organization needs to be pursued. (ISO 31000:2009, 9) Integration of ERM features at all levels of organization can be enhanced by strong visible executive leadership (Branson 2010).

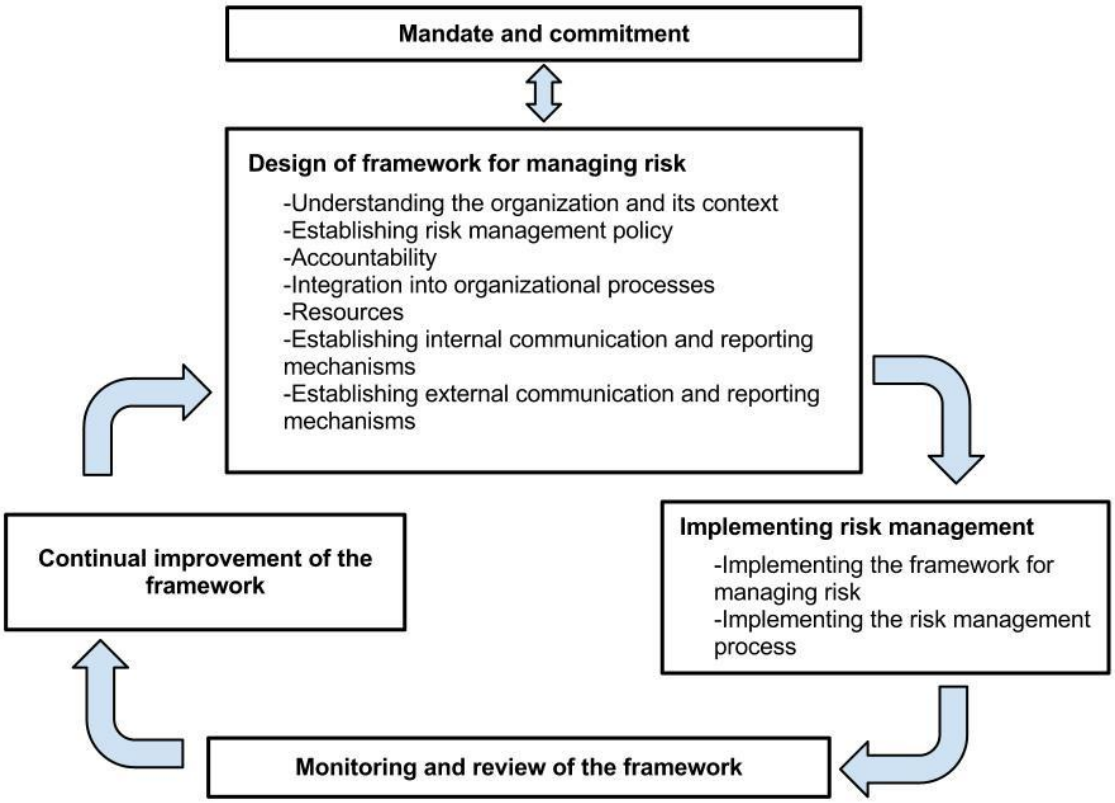


Illustration 7: The framework for managing risk

ISO 31000 highlights the importance of considering stakeholders and accordingly emphasizes their inclusion into risk management activities. Stakeholders include internal and external stakeholders. In every decision and activity, appropriate communication and consultation should be practiced continually. Establishing communication procedures will assist in identifying the stakeholders' perceptions, building reputation and gaining valuable information related to management of risks. (ISO 31000:2009, 12; Kloman 2008, 35-40)

The risk management framework is built upon continual re-evaluation and improvement. Typically, the internal audit function of the organization is supposed to participate in estimating the effectiveness and efficiency of risk management (Branson 2010; Institute of Internal Auditors, 2010). Effectiveness and relevance of RM framework and RM activities are to be

monitored and adjusted to changing conditions in the operating environment (Kloman 2008, 77-78).

In designing the framework for managing risk, several elements need to be taken into account:

1. Understanding the organization and its context;
2. Documentation of risk management;
3. Accountability;
4. Integration into organizational processes;
5. Resourcing; and
6. Internal and external communication and reporting mechanisms.

Risks are managed in the context of the organization, which includes the *external* and *internal context* (ISO 31000:2009, v). For comparison, COSO ERM (2004, 2) recognizes only the internal environment as an area of consideration in managing risk. "External context" is somewhat equivalent to more mainstream expressions of "operating environment" or "business environment". The width and depth of evaluating the external context depends on the organization and its capabilities. ISO 31000 sets no exact requirements for what should be evaluated, but lists some typical aspects, such as socio-cultural environment, trends, and perceptions and values of stakeholders. The *internal context* should encompass all the organizational features relevant to the RM. As contemplated later in chapter 3.3.4, the internal and external context need to be assessed with regard to RM process as well.

ISO 31000 classifies stakeholder groups into *internal* and *external stakeholders*. Although not directly stated, the standard most likely uses "*internal stakeholder*" to refer to employees of the organization. Correspondingly, "*external stakeholder"* is used to refer to other stakeholder groups, such as customers, suppliers and officials. The division to internal and external stakeholders serves the purpose of recognizing different categories of stakeholders, who have different needs and implications with regard to organization. However, the division based on legal entities or ownership is not always the most fluent, since the efficiency of the value network may require extended exchange of information. Therefore, it may be difficult to distinguish between the internal and external stakeholders.

Systematic and integrated approach to RM requires documentation in various areas. Organizational efforts to achieve objectives are guided by *RM policies* and *RM plans*. Relevant information, such as controls and consequences, about individual risks are recorded in *risk register* (ISO Guide 73:2009, definition 3.8.2.4). RM activities and decision making should be accordingly recorded in order to enhance improvement of organization. Furthermore, in assessing risks, recorded data on past decisions can be of assistance (ISO 31000:2009, 21; Shortreed 2010).

ISO 31000 regards risk management policy as a written "*statement of the overall intentions and direction of an organization related to risk management"* (ISO Guide 73:2009, definition 2.1.2). The contents of the RM policy can be defined by the user. Typically, an organization has RM policies for different areas of RM, most important of which are (Shortreed 2010)

1. Policies regarding RM framework
2. Policies regarding RMP
    a. Policies on risk appetite
    b. Policies on risk criteria
3. Policies regarding risk communication

Different RM policies should be regularly reviewed and adjusted to changing conditions. *RM framework policies* are usually public documents that outline main aspects of the organization's RM. This is equivalent to what ISO 31000 regards as the *risk management policy*. The RM framework policy is typically a short public document, which states the main characteristics of the organization's RM, including the accountabilities, context of RM and terminology. (Shortreed 2010)

RM decisions should be guided by written policies in order to determine *risk appetite*, *risk criteria* and risk reporting. *Risk appetite* is defined in ISO 31000 as "*amount and type of risk that an organization is willing to pursue or retain*" (ISO Guide 73:2009, definition 3.7.1.2). In each RM process, risk appetite is expressed in *risk criteria*, which are the "*terms of reference against which the significance of a risk is evaluated*" (ISO Guide 73:2009, definition 3.3.1.3).

Risk appetite should be determined in two dimensions: firstly, an organization should define its risk appetite for a "business-as-usual" scenario, i.e. a condition that can be expected to persist, a "normal" situation. Secondly, risk appetite should be determined for a worst-case scenario. In situations where statistical probabilities can be applied, such as in case of financial risk, a popular method for measuring worst-case scenarios is Value-at-risk[22], which will express the worst-case loss in a given probability, typically at 95% confidence level. This indicator can be used to evaluate aggregate risk with current or prospective financial situations (Linsmeier & Pearson 2000). However, worst-case scenarios as well as "business-as-usual" situations can also be evaluated qualitatively. This may be the only option, for instance in situations, where sufficient statistical data is unavailable or statistical data cannot be applied. (Shortreed 2010)

Risk criteria are based on objectives of the organization as well as external and internal context (ISO Guide 73:2009, definition 3.3.1.3). In determining the risk criteria, organization needs to consider mandatory requirements by legislation, and other country- or industry-specific regulators. In addition, organizations are presumed to comply with informal normative behaviour set by the operational environment. This includes among others business ethics, environmental issues, and sustainability. Official mandatory requirements are often formulated with quantitative specifics, making it easy to evaluate compliance with them. On the contrary, informal expectations, such as ethics, may not be as unambiguous to comply with. This creates a challenge for the formulation of RM policy regarding the risk criteria. (Shortreed 2010)

A *risk reporting policy* is a guidance on how risks are presented in an aggregated from, when reporting risks to senior management and other units. Instead of presenting a series of individual risks, it may be sensible at some occasions to present risks in aggregated form, especially in terms of low-level risks. However, the procedure of aggregation needs to be harmonized with according organization-wide instructions. Without general agreeement and guidance on aggregation, risk information may be at worst misguiding. For example, in situations, where a risk is divided into smaller components, which are examined as individual risks, the total risk

22 *VaR*

involved may exceed the risk criteria, whereas the components as individuals may not be significant enough to justify additional risk controls. (Shortreed 2010)

Implementing RM as an integral part of organizational processes needs to be demonstrated in a *risk management plan*, which according to the ISO Guide 73:2009 is a *"scheme within the risk management framework specifying the approach, the management components and resources to be applied to the management of risk"* (ISO Guide 73:2009, definition 2.1.3). Large organizations can apply many RM plans at different hierarchies, such as individual projects or processes, but there should always be an organization-wide plan as well. Furthermore, RM framework should be periodically evaluated against the RM plan (ISO 31000:2009, 11-13; Purdy 2010). Chosen risk treatment methods and according monitoring measures are specified in a *risk treatment plan* (ISO 31000:2009, 20).

ISO 31000 requires that RM should be seamlessly integrated into organizational processes (ISO 31000:2009, 11). In other words, the RM system should be adjusted to existing management practices. Due to this reason, ISO 31000 is not certifiable; An individual management structure can not be certified as right or wrong. Despite not being certifiable, any organization can be audited against the main principles of the standard. The requirements set by ISO 31000 are qualitative, thus making it impossible to unambiguously detect deviations from it.

The integration is facilitated by sufficient training, resourcing and communication (Shortreed 2010) In addition, as stated earlier, strong commitment and leadership from the management is required (Branson 2010). Taking RM as a part of everyday management and processes of organization requires RM to be relevant and value-adding, and this ability to be effectively communicated to stakeholders. In addition, internal stakeholders need to be assured, that RM is not merely about achieving compliance with corporate governance requirements, but actually an everyday tool of making better informed decisions aligned with the goals of the whole entity.

An ISO 31000 -based RM framework is partially facilitated by full accountability on risks. *Accountability* refers to designation of *risk owners* for each risk. *Risk owner* is an employee, which will be accountable for managing certain individual risk (ISO Guide 73: 2009, definition 3.5.1.5). In addition to knowing who is accountable for managing the individual risk, ISO 31000

also requires to ensure appropriate authority and competence to proceed with managing risk. To support fulfillment of full accountability, RM performance needs to be measured and successful efforts rewarded appropriately. Furthermore, it is necessary to identify, who is responsible for development, maintenance and implementation of the framework for managing risk. (ISO 31000:2009, 11)

To function as expected, RM requires sufficient resources for various functions, most important of which are stated as follows (ISO 31000:2009, 11):

1. people, skills, experience and competence;
2. resources needed for each step of the risk management process;
3. the organization's processes, methods and tools to be used for managing risk;
4. documented processes and procedures;
5. information and knowledge management systems; and
6. training programs.

(1.) and (6.) are staff-related requirements, whereas (3.), (4.) and (5.) consider formal structures of risk management. Efficient RM needs both effective RM framework and skilled labour force. (2.) holds potential for significant costs. Depending on the RMP, assessment and treatment of the risk can be a cause of remarkable expenses, for instance, in terms of acquiring insurance coverage for a large manufacturing plant. RM expenses should not be budgeted as separate RM expenditures, but they should instead be appropriately allocated to corresponding business units or functions (Shortreed 2010).

Appropriate *communication and consultation* (ISO Guide 73:2009, definition 3.2.1) are an integral part of a successful risk management framework. The purpose of communicating the RM framework is to keep stakeholders aware of all the relevant aspects of an organization’s RM framework. Sufficient communications are vital especially when implementing changes to the RM framework. (Shortreed 2010)

The communication needs vary between the two stakeholder categories. Internal communication mechanisms are to ensure efficient communication of (ISO 31000:2009, 12)

- key components of the RM framework and subsequent modifications;
- effectiveness and outcomes of RM framework; and
- relevant and timely information derived from application of RMP.

Correspondingly, sufficient consultation mechanisms with external stakeholders need to be established and maintained. ISO 31000 regards communication with external stakeholders to involve (ISO 31000:2009, 12)

- engaging appropriate external stakeholders and ensuring an effective exchange of information;
- external reporting to comply with legal, regulatory, and governance requirements;
- providing feedback and reporting on communication and consultation;
- using communication to build confidence in the organization; and
- communicating with stakeholders in the event of a crisis or contingency.

Consultation is defined as two-way communication with stakeholders in order to assist decision making. "Consultation" is also used in the concept "*consultative team approach"*, which most likely refers to the utilization of various stakeholders' expertise and consideration of their interests (ISO 31000:2009, 14). ISO 31000 highlights that risk information should be consolidated from a variety of sources to ensure that many diverse perspectives on the specific risk can be taken. In case of both internal and external stakeholders, ISO 31000 encourages to identify their perceptions of risk (ISO Guide 73:2009, definition 3.2.1).

3.3.4 Risk Management Process

Clause 5 of ISO 31000 defines the risk management process as "*systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring and reviewing risk*" (ISO Guide 73:2009, definition 3.1). The main goal of RMP is to modify risks to correspond risk criteria and monitor that they will remain within the criteria. RMP should be used in every decision in organization. However, this does not indicate that RMP should be a laborious

uniform procedure, but rather to be adjusted to the context of risk and to apply risk management efforts in an appropriate scale. (Shortreed 2010)

As shown in Illustration 8, the RMP is a three step procedure of

1. establishing the appropriate context for RM;
2. assessing the risk; and
3. treating the risk.

The components of the above-mentioned illustration are presented and examined in this chapter and the following chapters 3.3.4.1 and 3.3.4.2.

Throughout the RMP appropriate *communication and consultation* with stakeholders is practiced. ISO 31000 states that communication and consultation should be practiced "*during all stages of the risk management process*" (ISO 31000:2009, 14). This is explicitly illustrated in the above portrayal of RMP. At first this precept might seem to be excessively burdensome, but it makes sense when taking into account the principle, that ISO 31000 is to be tailored to the needs of the organization. That is to say, communication and consultation, as well as every other aspect of ISO 31000 should be economically justifiable, or in other words, performed in a meaningful scale. Monitoring and reviewing the RMP is facilitated by recording risk management procedures. By establishing sources of information about RM decisions, future RM activities and improvement of the framework can be greatly assisted (ISO 31000:2009, 21).

In evaluating the context of RMP (*establishing the context*), the risk manager needs to take into account the external and internal context, as in the case of risk management framework, although in greater detail. In addition to internal and external context, the *context of the risk management process* needs to be defined for each risk. *Context of the RM process* is a description of all the relevant aspects related to the management of risk, such as objectives, timing and location of the particular RMP. (ISO 31000:2009, 16) This includes at large the same details as the risk management plan.

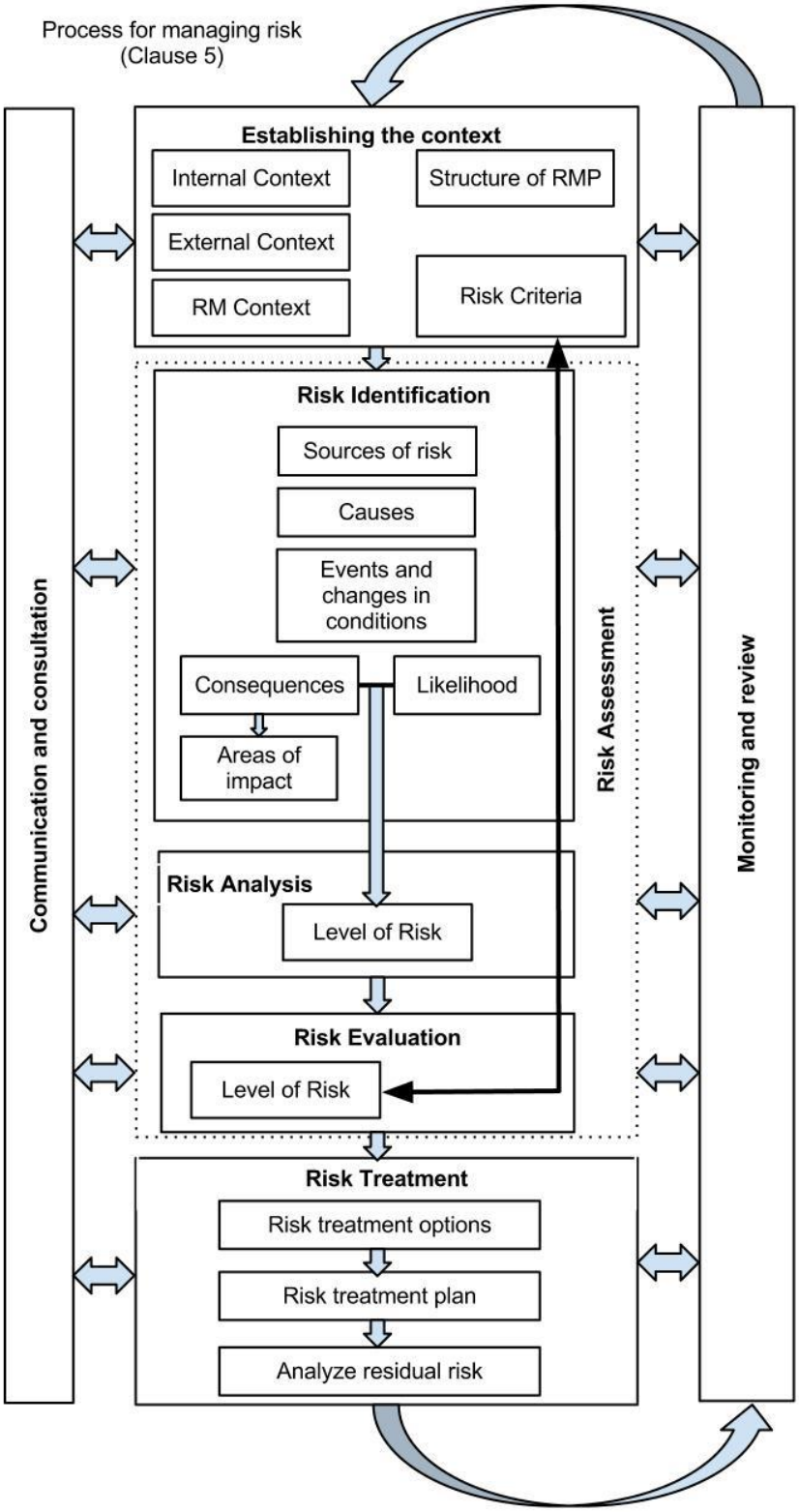


Illustration 8: The risk management process

The main output of establishing the context of managing risk are the "*risk criteria*", which are the "*terms of reference against which the significance of a risk is evaluated*" (ISO Guide 73: 2009, definition 3.3.1.3). In other words, if the level of a risk exceeds a certain threshold derived from the risk criteria, measures to modify risk are needed. *Risk criteria* are affected by organization's *risk appetite* and *risk tolerance*. *"Risk tolerance"* is defined as *"organization's or stakeholders' readiness to bear the risk after risk treatment in order to achieve its objectives"* (ISO Guide 73:2009, definition 3.7.1.3).

Shortreed (2010) concludes that "tolerance" is used in a situation, where a risk cannot be further modified to an acceptable level, but nevertheless is retained in order to achieve objectives. This is indeed what ISO 31000 suggests, although does not directly state. This semantic differentiation of "acceptable" and "tolerable" risks may be meaningful with regard to those cases, where the formal risk criteria can not be used as a reference, for example because the risk criteria need to be updated to correspond the new situation. Herein the message of ISO 31000 is the following: formal risk criteria should not always be slavishly obeyed. Moreover, since these two concepts have been "confused" and "misused" in RM literature (Purdy 2010), it may have been reasonable to bring up a formal definition for these concepts. Purdy's observation is supported by a recent review of corporate governance in financial sector, which concludes that there is no consensus in that sector about the meaning and difference of *risk appetite* and *risk tolerance*" (Basel Committee on Banking Supervision 2010).

3.3.4.1 Risk Assessment

Risk assessment consists of three consequent steps, purpose of which is to compose a comprehensive list of possible risks (*risk identification*), examine their qualities (*risk analysis*) and based on the examination to find out, whether the risk is acceptable or not (*risk evaluation*) (ISO Guide 73:2009, definition 3.4.1). One of the volumes of the current ISO 31000 family, *Risk Assessment Techniques*, is namely dedicated to sharing practical guidance on using risk assessment techniques. The guide includes a selection of widely used practical methods for each step of risk assessment process. However, these risk assessment techniques are not examined in this study, since they are not essential in terms of scientific examination of ISO 31000.

Risk identification in ISO 31000 is defined as *"process of finding, recognizing and describing risks"* (ISO Guide 73:2009, definition 3.5.1). Risk identification is about creating a comprehensive list of risks facing the organization. It involves finding out *"sources of risk, areas of impact, events (including changes in circumstances) and their causes and their potential consequences"* (ISO 31000:2009, 17).

"Risk source" refers to a tangible or intangible element which has a potential to give rise to the risk (ISO Guide 73:2009, definition 3.5.1.2). "*Event"* refers to an occurrence or a change in circumstances (ISO Guide 73:2009, definition 3.5.1.3). Although not determined in the vocabulary, "*cause"* refers to a cause of an event (e.g. ISO 31000:2009, 17). Correspondingly, *consequence* refers to an outcome of an event affecting objectives (ISO Guide 73:2009, definition 3.6.1.3). *Area of impact* is namely the area (e.g. part of organization, department of a manufacturing plant, etc.) on which the consequences of an event affects.

Risk identification should enlist risks, whether or not their source is under control of an organization. Identified risks are placed in a *risk register*. Especially in the situation, where there are many uncertainty factors related to the identification of risk, an thorough estimation should be made including a variety of possible risk sources, events and their causes, and consequences. Identification of risks should also take into account the knock-on -effects of consequences, i.e. the consequences of the consequences.

When meaningful, a large quantity of equivalent risks can be aggregated, which is to say, to be examined as a single corpus of similar risks. This applies especially to the risks with a high probability, such as shoplifting in case of retail business. The challenge in identifying risks is to accumulate and utilize relevant information to gain an insight of the current and possible future risks facing the organization. (ISO 31000:2009, 17)

Risk analysis is performed to each risk identified in the previous step of risk assessment process. The analysis aims at determining the *level of risk* (ISO Guide 73:2009, definition 3.6.1.8), which is an indicator of magnitude of risk. Level of risk is defined as a combination of *consequences* and their *likelihood*. Based on the level of risk, the organization will be able to define its stance to

the particular risk, which is to say, whether the risk is acceptable or not. In case of being unacceptable, the risk needs to be modified to correspond the acceptable level of risk.

There is a vast quantity of different methods of risk analysis, utilizing both historical data and future predictions. ISO 31000 encourages the risk manager to find suitable methods for each risk. An example of a risk analysis tool is risk matrix, which uses a matrix in depicting different risks and their seriousness as an outcome of two factors, consequences and likelihood (ISO Guide 73:2009, definition 3.6.1.7). Risk analysis can be performed with "*varying degrees of detail*". Herein factors to be taken account of are costs, availability of data, methodological meaningfulness regarding the nature of risk, and uncertainties and inaccuracies related to modelling of risk. Depending on the purpose, risk analysis can be qualitative, semi-quantitative or quantitative or a combination of these. Furthermore, risk analysis can be objective or subjective, thus taking account the relevant stakeholders' perceptions of risk. (ISO 31000:2009, 18)

As in ERM, ISO 31000 encourages to take a portfolio view on risks. Therefore in analyzing risks the interdependence of the risks need to be assessed. Leitch (2010) considers this an improvement when compared to risk register -driven RM processes. Focus on risk registers includes an inherent danger to consider single risks per se, without taking the wider context into account. (Leitch 2010)

In order to determine the acceptability of a risk, the level of risk needs to be compared to the risk criteria set in the beginning of the RMP cycle. In addition to risk criteria, the *evaluation of risk* is affected by organization's *risk attitude*, which is described as *"organization's approach to assess and eventually pursue, retain, take or turn away from risk"* (ISO Guide 73:2009, definition 3.7.1.1). Based on this definition, *risk attitude* refers to a cultural characteristic of an organization. However, it is unclear, why ISO 31000 defines risk evaluation with regard to risk attitude, since in determining risk criteria, the internal context, including the culture, has already been taken into account.

3.3.4.2 Risk Treatment

After evaluating the level of risk with regard to risk criteria, risk treatment includes selecting the appropriate *controls*, which are measures to modify risk (ISO Guide 73:2009, definition 3.8.1.1). If the existing risk controls are not sufficient, then risk is modified with a treatment option. Effectiveness of a risk treatment is then evaluated and the *residual risk* is compared to risk criteria and decided whether it is acceptable or not.

However, as Purdy (2010) noted, this procedure produces a logical dilemma in the situation, where further risk management procedures would be meaningful on a cost-benefit basis, although based on the established risk criteria the risk is already at an acceptable level. If one wishes to follow ISO 31000 word for word, no further risk treatment would be needed, even though it would prove to be financially beneficial. (Purdy 2010)

A RMP can include several different risk treatments, all of which in combination should modify risk to an acceptable level. Naturally that is not always the result and in some cases risk may not be modified to an acceptable level. In this case, the risk becomes "tolerable" (see discussion in chapter 3.3. Risk treatment options presented by ISO 31000 (ISO 31000:2009, 19) include:

a. avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
b. taking or increasing the risk in order to pursue an opportunity;
c. removing the risk source;
d. changing the likelihood;
e. changing the consequences;
f. sharing the risk with another party or parties (including contracts and risk financing); and
g. retaining the risk by informed decision.

Traditionally, four distinct archetypes of risk treatment options have been recognized (e.g. Crouhy & Galai, & Mark 2005, 2; Laurila 1981, 15) as follows:

1. removing the risk;
2. mitigating the risk;
3. retaining the risk; and
4. sharing the risk.

The selection of risk treatment options in ISO 31000 is basically the same than the traditional four archetypes, with a few different points of emphasis. The concepts are correspondent as follows:

- (1) corresponds (a) and (c);
- (2) corresponds (d) and (e);
- (3) corresponds (b) and (g); and
- (4) corresponds (f).

Risk treatment options should be chosen using the best available information, but taking into account the cost-to-benefit ratio of the implementation. In addition, legal and regulatory requirements, and business ethics -related aspects should be considered. Furthermore, risk treatment itself can introduce risks and secondary risks, which should be incorporated in the processing of the original risk. Risk treatment is documented in a *risk treatment plan*, which should include all the relevant details, such as chosen treatment options, performance measures and schedule (ISO 31000:2009, 29).

3.4 Criticism

Since the publication of ISO 31000 in November 2009, only a few academic reviews of the standard have been published. In this section two critical reviews by Leitch (2010) and Aven (2011) are presented with according points of criticism. The two reviews are partly overlapping with regard to terminological critique, but have different overall focuses. Whereas Leitch also criticizes the functional problems inherent in ISO 31000, Aven concentrates solely on semantic

issues and presents some suggestions to reformulate current definitions in order to achieve a more coherent standard. Terminology has constituted a problem also for the earlier RM standards (Ale et al 2010).

Leitch's (2010) overall approach to ISO 31000 is excruciatingly negative. He argues that ISO 31000 is destined to fail, since it

1. is unclear;
2. leads to illogical decisions;
3. is impossible to comply with; and
4. is not mathematically based.

The first three topics are reviewed in following sections of this chapter. The fourth topic can be addressed by fact, that the work group behind ISO 31000 has intentionally taken a broad approach to defining likelihood related to risk. Likelihood can be defined in a way that is most convenient and meaningful regarding the RMP, whether it be quantitative or qualitative. (ISO 31000:2009, 18) As Raz and Hillson found out in their study, for some reason the generic RM standards tend to disfavour quantitative risk assessment methods (Raz & Hillson 2005).

Leitch (2010) and Aven (2011) argue that ISO 31000 does not perform well on all occasions in defining RM terminology. Some customary terms are by his opinion, unnecessarily redefined. However, since one objective of RM standards is to give uniformity to the vocabulary used in the field of RM, in some cases it may be unavoidable to forge the old customary definitions anew. The definition of "risk", according to Leitch, is problematic, since it binds risk into objectives, which in some cases may be undefined. This would result in a logical error, because without objectives there should be no risk. In addition, the focus on objectives is subject to possibly misguiding the managerial effort to achieve separate sub-objectives instead of finding the overall best solution. However, objectives may not always be conscious. For instance, "survival" may be an objective as well, even though pursuing it would be purely subliminal. (Leitch 2011; Aven 2011)

Furthermore, Leitch (2010) asserts that although ISO 31000 has formally embraced a “neutral” view on risk, with according recognition of both upside and downside (see discussion in chapter 3.3.1), the standard on many occasions still reflects the old loss avoidance -based approach to risks. Interestingly, in their analysis of recent RM standards, Henriksen & Uhlenfeldt (2006) argue that RM standards, with the exception of AS/NZS 4360:2004, also suffer from dysfunctional implementation of the concept of “risk” as two-sided phenomenon. Since ISO 31000 is mostly built upon AS/NZS 4360, it is curious, why Leitch and Henriksen & Uhlenfeldt have ran into different conclusions.

The RMP of ISO 31000 has a serious flaw in the case where a risk is already tolerable, i.e. within the limits of the risk criteria. In such situations ISO 31000 suggests that no risk treatment is needed, even if additional modifying measures should prove to be beneficial on cost-benefit basis. The same problem has also been addressed by Purdy (2010). Risk aggregation is another problematic area. Since no guidance on risk aggregation is provided, an ISO 31000 -compliant RMP may lead to illogical decisions in case of unsuitable aggregation of risks. An example of such is a situation, where risk is disaggregated into multiple small fragments, with each fragment insignificant enough to be acceptable when examined through the risk criteria, but when been taken into account as an aggregated risk, constitute a problem to be addressed. (Leitch 2010)

Also, Leitch claims that ISO 31000 sets “idealistic requirements” for organization, making compliance impossible. Such is the case with, for instance, continual review of risk criteria. However, an important note should be made that any area of ISO 31000 may become excessively laborious if the organization does not relate the scope and width of risk management tasks to its needs. Indeed, not every risk should be made a board-level issue and not every change in the operational environment is a cause of redefinition of risk management policy. ISO 31000 will provide the principles as the foundation for good risk management practices. This is also its inherent challenge: the standard does not provide ready answers.

However trivial some remarks regarding the RM terminology may seem, the concern is justifiable. Vagueness of terminology greatly reduces the applicability of a standard, thus thwarting its attempt to harmonize risk management. On the other hand, others believe, that the minor problems will not constitute an insurmountable hindrance for the success of the standard

(e.g. Väisänen 2011) Very little scientific research on ISO 31000 and its terminology has been done so far. Therefore, an exhaustive conclusion on the success of the standard can not be made. Any major effort to establish a global best practice in risk management, such as in case of ISO 31000, will undoubtedly stir up criticism as well as praise. Further debate on the new standard will surely emerge among the scientific community and risk management practitioners.

3.5 Challenges of Implementation

The first of the *Principles* in ISO 31000 emphasizes risk management as a value-preserving and value-adding function for the organization. However, this is not always the case, when risk management is not used, as ISO 31000 suggests, a tool for decision making. In case of compliance-oriented perception on risk management, focus is placed on internal controls. In addition to bringing (sometimes false) psychological comfort, this approach may encourage risk-aversive behavior among the general management (Kloman 2008, 76; Power 2009).

Risk management, as well as organization as a whole, needs to incorporate continual review and monitoring as an inherent attribute. Especially in the smaller organizations the lack of systematic approach constitutes a problem, as the administrative tasks are often neglected due to the lack of time and monetary resources. Nevertheless, this is not merely a specific problem of risk management, but any strategic-level planning which is easily substituted by more acute day-to-day tasks.

Whether RM is considered throughout the organization as a value-adding process depends on the risk culture. Risk culture is partly built upon mutually agreed terminology. A strong initiative to remove outdated perceptions on “risk” should be made. An example of such unwelcome implications is the consideration of “risk” as the management of adverse events. As risk management is employed by several different professions, their deep-rooted perceptions may be a hindrance to the terminological harmonization. The role of the torchbearer for promoting better risk culture typically belongs to the risk manager, who operates with the mandate and assistance of the senior management and the board.

Furthermore, it is probable, that the prevailing method of practicing one-way communication with stakeholders is a major hindrance in achieving compliance with ISO 31000. Despite major

leaps forward with the increased use of social media, it is yet probable that organizations do not fully utilize genuine two-way communication and consultation. This would require change in attitudes towards transparency as a cornerstone of trust (Kloman 2008, 85-86).

The problems in the above-mentioned areas, namely (1) value-addition, (2) systematic and continual approach, (3) risk culture, (4) terminology and (5) communications are likely to be present in the results of this present study. Among others, these areas are measured in the questionnaire used in this research project. The method for the research is reviewed in greater detail in the subsequent chapter.

4 RESEARCH METHOD

To address the research questions outlined in chapter 1.3, the RM maturity of Finnish organizations was measured by conducting a survey based on the contents of the standard. Some authors imply that an organization's risk management should be reflected against the benchmark criteria set by the *Principles* and *Attributes of enhanced risk management* of ISO 31000 (Shortreed 2010). However, in this study, a more in-depth perspective into the components of the RM maturity was taken. Thus, the above-mentioned elements of RM maturity were not used *per se*, but their contents were operationalized into a series of more detailed questions. However, the set of questions used in this study is merely one interpretation about the necessary elements to measure RM maturity through ISO 31000.

The survey was self-administered, and for the most part structured, although a few opportunities for open responses were added in to gain a wider perspective on the challenges related to the particular area of risk management. However, this was done knowing that in self-administered surveys open-ended questions are often not useful for measurement, but on the contrary, their results are mostly anecdotal (Fowler 2002, 62 - 63).

The questionnaire included 37 claims on the state of risk management, with a Likert scale answer option. The answer was required on a 1 to 5 scale, wherein 1 represented as "Totally disagree" and 5 correspondingly "Totally agree". Fowler (2002, 85) suggests adding a "don't know" -option, when it is likely that a large number of respondents are not familiar with the topic. In this study, the option was not included, since presumably the voluntary respondents were well aware of the state of the RM in their organizations.

The web-based survey was built on Google Docs platform, using the Google Form tool. Link to the survey was posted on the web pages of three Finnish risk management -related organizations: FinnRiMa, Finnish Institute of Internal Auditors and Turvallisuus & Riskienhallinta[23] -magazine. In addition, the intention was to directly contact the readers of the Turvallisuus & Riskienhallinta

[23] in English: *Security and Risk Management*

–magazine by email. However, due to the suddenly emerged problem with regard to personal data privacy, this channel could not be applied, which reduced the total amount of responses.

The survey was accessible for anyone with an access to Internet and according web pages. Nevertheless, it is presumable that the survey attracted relevant respondents, since the web pages were highly specialized in risk management -related areas. In addition, in the context of this study, it is not likely that Internet as the sole survey medium would have framed a significant number of relevant respondents out of the study, as may be in case of some focus groups (Fowler 2002, 74).

For the sake of clarity, the survey was conducted in Finnish. This would presumably eliminate possible language-related misunderstanding regarding the meaning of the questions. Since the web pages were targeted to Finnish-speaking audience, the most convenient option was to conduct the survey in Finnish as well. However, herein lies the chance for a error in terms of translating English terminology into Finnish. Moreover, as stated above, the diversity of risk management terminology results in difficulty of finding common understanding on terms and definitions. This applies to both English and Finnish RM terminology.

The non-probabilistic sampling method used in this study limits the choice of statistical methods of analysis in order to evaluate the accuracy of the sample. This study required voluntary participation, which obviously biases the results, when compared to statistical sampling. No numerical probability can be assigned for an individual to answer the questionnaire. Thus, the attempt of this study is not to make a generalization on the main population based on statistical probabilities. (Fowler 2002, 37)

Fowler (2002, 95 - 100) lists four basic factors affecting the *validity* of the survey questions: The respondents:

1. do not understand the question;
2. do not know the answer;
3. cannot recall the answer, although they know it; or
4. do not want to report the answer.

The first problem (1.) can be addressed with explicit formulation of the survey questions. Since the survey is targeted to RM professionals, it is likely that the respondents possess a good knowledge of RM. However, as stated earlier, since RM is a field with diverse heterogeneous terminology, vocabulary-related issues may pose a threat to correct understanding of the questions. (Fowler 2002, 81 - 84, 96)

In the context of this present study, the respondent's background is likely to achieve how he perceives RM. For instance, security or insurance professionals may see risk management from loss avoidance -perspective, whereas internal auditors tend to emphasize compliance with corporate strategy. It is important to consider that "risk management" can also be perceived as particular function of an organization, such as risk manager or RM department, with an overall responsibility of all risk management in an organization. However, in the context of ISO 31000 and ERM, risk management is regarded as an integrated function and part of all decision making. Therefore, the variation of meanings with regard to the concept of "risk management" and other related terms needs to be taken into account when formulating the survey questions. (Väisänen 2011)

The second problem (2.) is related to the basic assumptions behind this study, namely that the survey respondents are capable of realistic reflection of the state of their organization's RM. The same method is widely used in RM-related surveys (e.g. Schrøder 2006; COSO 2010; Aon 2010; Accenture 2011). Thus, previous research papers support this methodological choice made in this study.

The third problem (3.) can be addressed by question formulation to enhance memorability, e.g. with mental cues. However, instead of trying to recall the exact answer, the respondents may instead use estimations to determine their "best-guess" response. The fourth point (4.) refers to social desirability, which is especially noteworthy regarding face-to-face interviews, but also to be considered in self-administered surveys. Questions that attempt to unveil sensitive information may result in nonresponse or erroneous results. The sensitivity of information is especially noteworthy in terms of enterprises operating in an environment of competition. This present questionnaire avoided too detailed an inquiry into risk maturity factors, which might prove to be too sensitive. In addition, the responses were anonymous. (Fowler 2002, 97 - 100)

In terms of composition, the questionnaire has two major elements: (1.) questions on the particular organization's background and (2.) questions on the factors of risk management maturity. Illustration 9 presents the composition of the questionnaire.

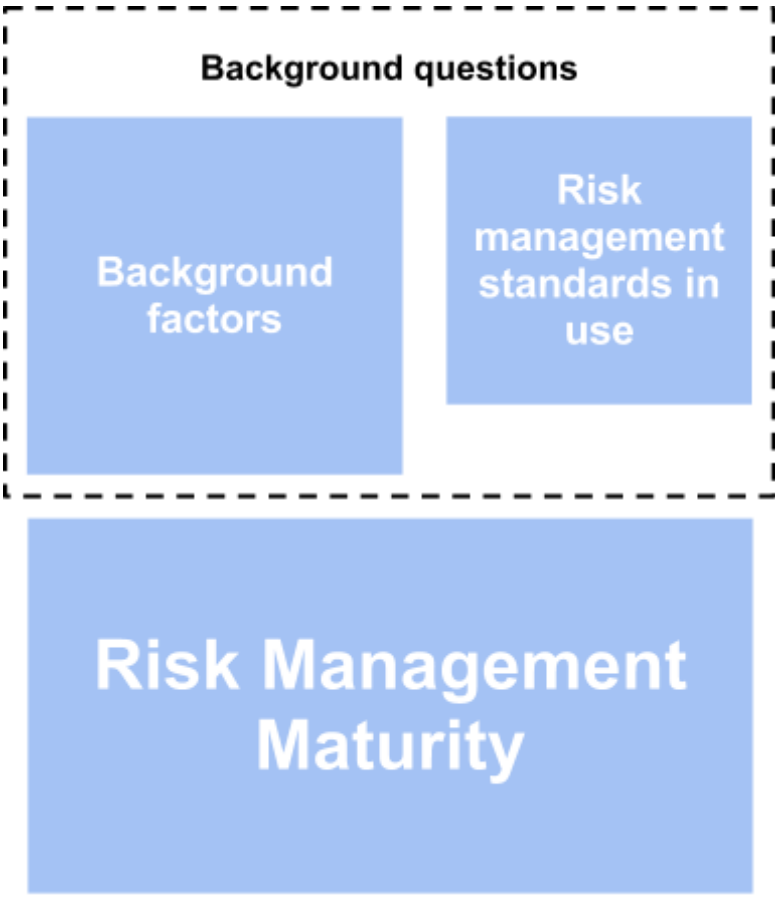


Illustration 9: The elements of the survey

The background questions were intended to encompass factors possibly relevant to the RM performance, such as size of the organization. These questions included:

1. field of activity (e.g. industry, wholesale);
2. number of employees;
3. annual turnover (if defined);
4. [for enterprises] being listed on Helsinki stock exchange (OMX Helsinki) or not;
5. respondent's profession;
6. respondent's work experience in RM-related duties.

In addition, the background questions investigated the level of awareness about ISO 31000 and risk management standards currently in use. These questions included:

1. RM standard used in the organization;
2. respondent's awareness of ISO 31000; and
3. plans to implement or not to implement ISO 31000.

The RM maturity part was divided into eight partly overlapping themes, which are reflected in ISO 31000. The structure of the questionnaire did not strictly follow the composition of the standard. The main purpose of the thematization was to establish thematic categories for a more convenient respondent experience. The amount of questions in each theme did not reflect the relative importance of the particular category.

Below are presented the eight different themes, in which the questions were classified. The according number of questions is presented in brackets ( ) after the title of the category.

1. Approach to RM (2);
2. Decision making (6);
3. Commitment of management (4);
4. RMPs (6);
5. Reporting of changes in operational environment (3);
6. Competences and accountabilities (3);
7. Information flows (12); and
8. Performance measurement and continual improvement (4).

The first theme (1.) was intended to shortly investigate, how RM is perceived in the organization. Unlike the other categories, in the first theme, Likert scale questions were not used. The second theme (2.) involved issues related to decision making, e.g. how well decision making would support achievement of objectives and whether the consequences of decisions are taken into account in an organization-wide perspective. The third theme (3.) encompassed evaluation of management and board commitment to RM.

Questions of the fourth theme (4.) included inquiries related to different stages of RMP, mostly with regard to risk assessment. Risk treatment -related issues were not considered in (4.), since meaningfully measurable aspects of risk treatment were covered in (2.). Actual risk treatment is fundamentally the same as decision making if risks are understood as opportunities, as the standard implies.

The fifth theme (5.) included the evaluation and reporting of changes in operational environment, namely the "external context". In the sixth theme (6.), the questions were related to accountabilities and competence in risk management. The seventh theme (7.) was exceptionally wide, with emphasis on information flows. This included among others the harmonization of terminology, two-way communications and documentation of risk management. In the final eighth theme (8.), continual reevaluation and improvement of RM framework was assessed.

Research on risk management maturity could have been conducted with other methods as well. The questionnaire could have been targeted to a multitude of an organization's employees, thus gaining a wider perspective on risk management maturity. However, this approach would bring in the problem of, whether other employees besides the risk manager are capable to evaluate the state of risk management besides of their own area of responsibility. If a reliable insight into risk management on many perspectives had been pursued, there would have been a need to create a multitude of different survey forms for each type of employee. The diversity of organizations and employee accountabilities would have constituted a major challenge for this approach. Therefore, in this study, a conscious decision was made to pursue simplicity via one single questionnaire form specifically targeted to risk managers.

Typically, when the objective of a study is to gain an in-depth view on an organization's risk management, a thorough audit procedure regarding the employees and formal structures is committed. The data accumulated by the chosen method, namely the questionnaire, is undoubtedly not as rich as could have been gained via audit procedure. Since the aim of this study is to draw conclusions based on a large number of organizations, an all-encompassing audit is not a viable option due to more extensive amount of research work needed.

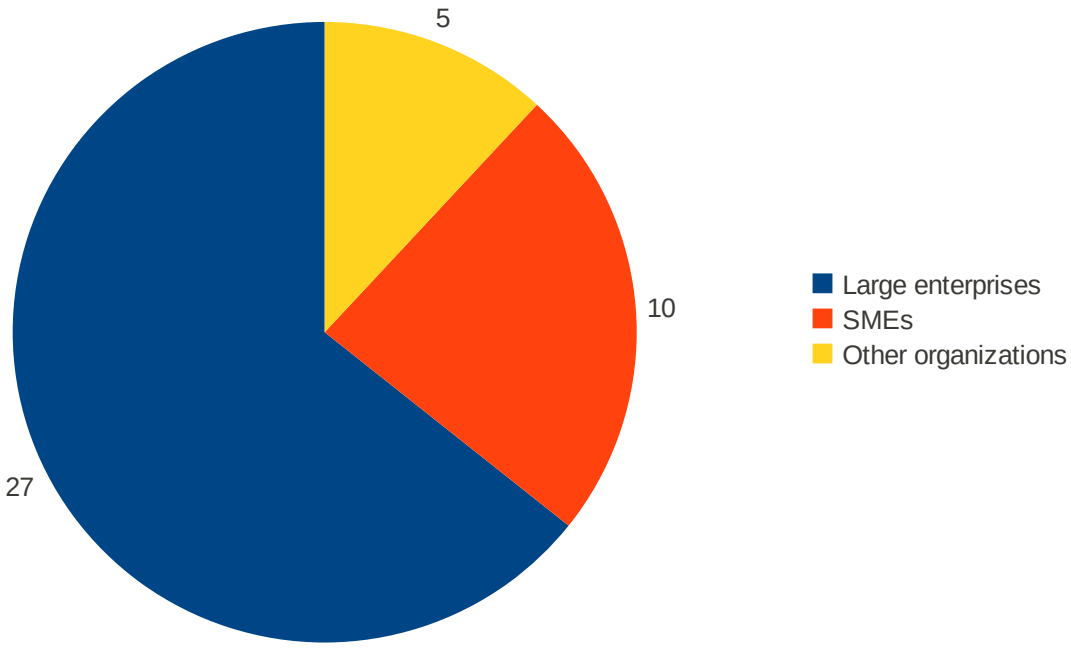
5 RESULTS & DISCUSSION

From all of the three sources, a total 42 answers were submitted, of which 27 were received via FinnRiMa and 15 via the remaining two sources. The total amount of responses can be regarded as satisfactory, since, as mentioned above, an important channel of data accumulation had to be left out due to privacy policy issues. Therefore, the results presented below should be regarded as directional. Furthermore, the large enterprises were over-represented in the sample, thus causing an upwards bias in the maturity scores.

Of all the respondents, 27 represented large enterprises and 10 small and mid-size enterprises[24]. The remaining five (5/42) respondents did not provide both turnover and number of employees to be identified as enterprises. It is likely that this category includes public sector and non-profit organizations, for which the annual turnover does not apply.

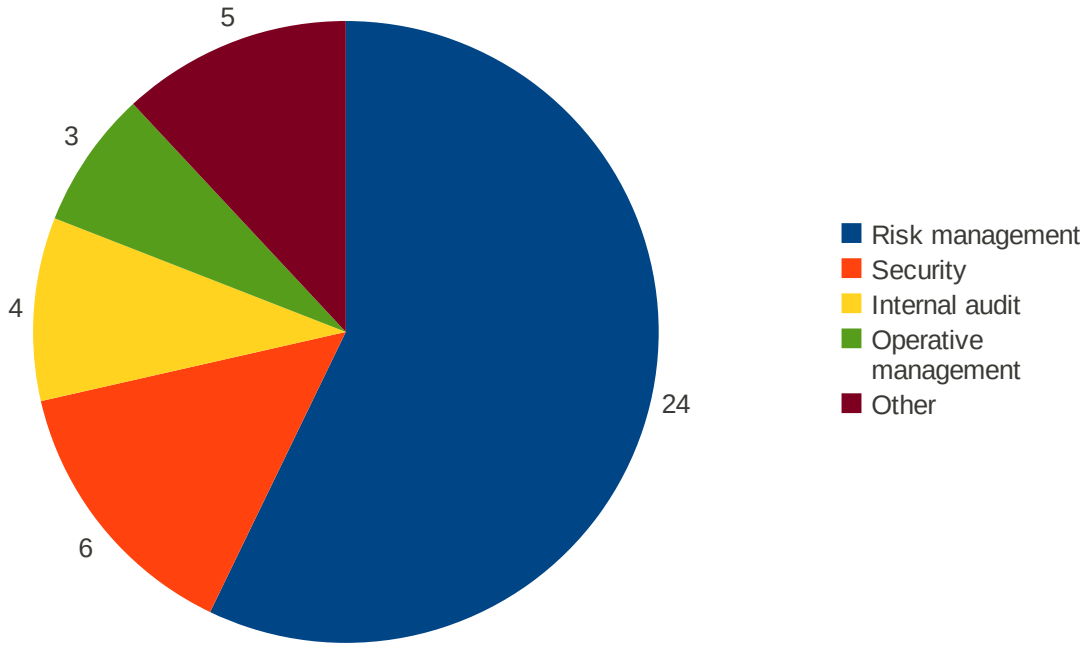
[24]SMEs consists of enterprises, which employ fewer than 250 persons and which have an annual turnover not exceeding EUR 50 million, and/or total balance sheet not exceeding EUR 43 million (European Commission 2003). In this study, SMEs were categorized by the annual turnover and the number of employees. The total balance sheet was left out of consideration, since it is presumably more difficult to recall.

Illustration 10: Relative proportions of different organizations, n = 42



The respondents represented very diverse areas of operation. Greatest individual categories represented were “manufacturing” (8/42 responses), “public administration and defence” (7/42) and surprisingly, “training” (6/42). The categorization, which was based on the Official Statistics of Finland (2010) classification of industries, apparently had too many different classes to choose from, thus resulting in scattered responses. Therefore, due to the relatively small number of answers even in the most frequently chosen classes, the response data was not analyzed by the area of operation of the organization. The analysis would have required a significantly larger number of respondents.

Illustration 11: B8: Number of respondents per primary work responsibility, n = 42



A vast majority of the respondents (24/42) indicated “risk management” as their primary work responsibility. Other job descriptions included “internal audit” (4/42), “security” (6/42), “operative management” (3/42) and “other” (5/42). With other classes besides of “risk management” attracting such a limited number of responses, it is not meaningful to compare respondent classes with each other. It is likely, that the category "risk management" had attracted responses from other categories as well, especially in the cases where a respondent is responsible for multiple work areas, e.g for both internal audit and risk management.

Of the 42 respondents 13 organizations used ISO 31000 and 12 organizations used COSO ERM in their risk management. This result was not in line with another recent ISO 31000 –focused survey, in which 21 out of 34 Finnish respondents reported the use of ISO 31000, whereas only 12 used COSO ERM (G31000, 2012). In this present study, the respondents could select more than one standard as their reference standard. The results indicate that a great portion of the organizations use several different standards in their risk management. The use of ISO 31000 and COSO ERM was at large overlapping, thus making it difficult to evaluate, whether the

performance of RM is a correlated with the use of the former or the latter standard. Furthermore, since the questionnaire included a possibility to select “self-developed model” as a reference RM standard, it is likely that this category also included the use of recognized standards with modifications. Those organizations that indicated utilizing solely ISO 31000 were extremely few in numbers. Therefore, this study can not meaningfully contribute to the interesting question of whether the use of ISO 31000 as a RM standard will contribute to the RM maturity.

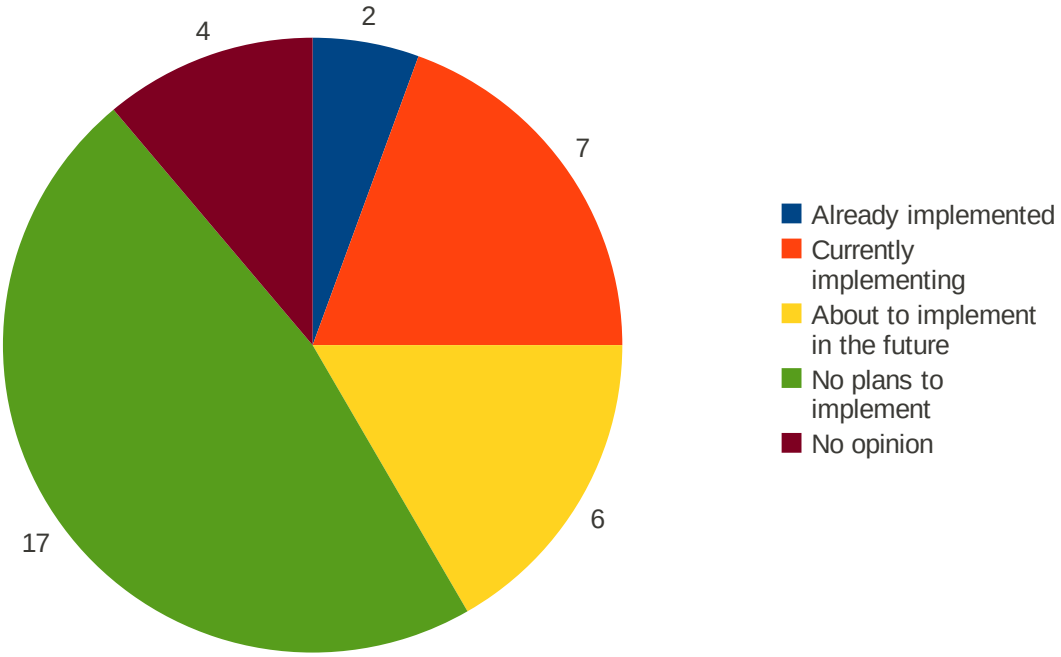


Illustration 12: B9: "Has your organization implemented ISO 31000?" n = 3

Approximately a quarter of the responses (9/36) indicated that the respondent’s organization had already implemented or was currently implementing ISO 31000 in their risk management. Six respondents had plans to adopt their risk management to the standard in the future. Nearly half of the respondents (17/36) expressed that their organization had no plans to implement ISO 31000 at all. More positive attitude towards the standard was recorded by the G31000 survey, in which more than half of the Finnish respondents reported to having implemented or being about to implement ISO 31000 in the future (G31000, 2012)

A note should be made, that the term "implementation" is ambiguous, when it comes to ISO 31000. The requirements set by the standard are qualitative, which means that every organization needs to find its own way how to benchmark its processes against the standard. The internal and external context of the organization determine, at what extent RM is practiced and with which tools. Therefore, there is no uniform way to "implement" ISO 31000. Some organizations may find it useful to harmonize their internal RM terminology with the terminology of ISO 31000, whereas the others may assess their operations against the Principles and Attributes of enhanced RM to determine the efficiency of their current RM architecture.

The two questions assessing the perception of "risk" and "risk management" revealed that approximately half of the respondents perceive these concepts in accordance to ISO 31000. More than half of the respondents (22/42) consider "risk" as an "effect of uncertainty on objectives", which is the ISO 31000 definition.

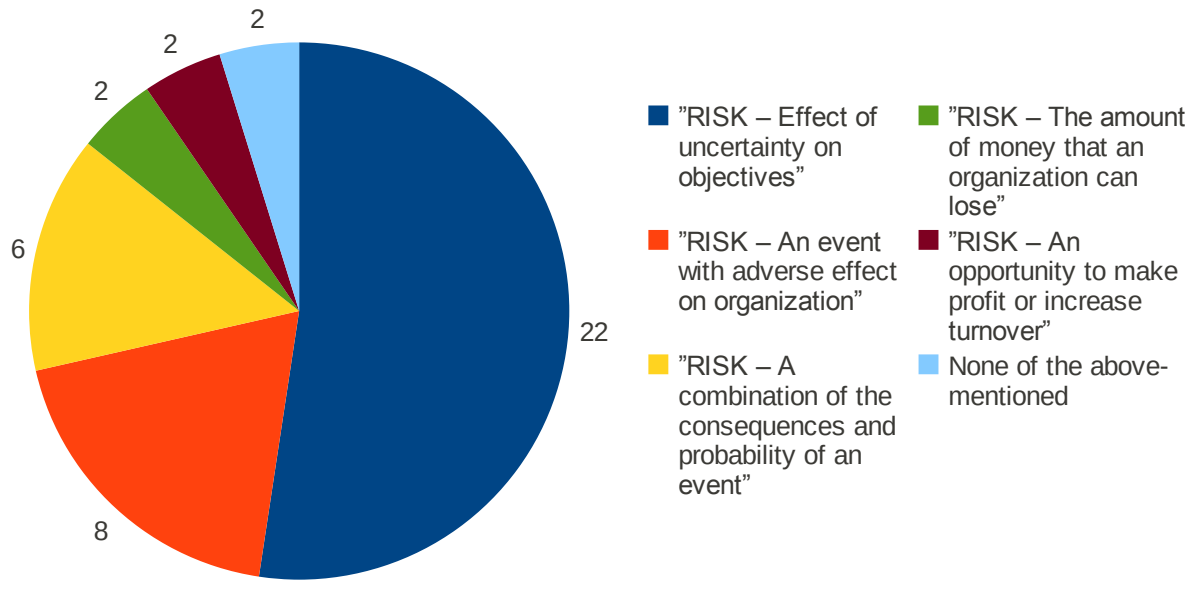


Illustration 13: B10: "Which ones of the following statements best describe your organization's orientation to risk management?" n = 42

The results of the question B11 also indicate compliance with ISO 31000 -based risk management. Approximately half of the respondents evaluate that their organizations' risk management is integrated in all decision making.

Based on the results of the preliminary questions B10 and B11, it may be concluded that RM principles of ERM and ISO 31000 are rather widely accepted. Nevertheless, a note should be made that an equally large proportion of respondents do not use or perceive risk management in compliance with ISO 31000. However, a more thorough view on the actual state of risk management can be gained by the responses to the questions assessing the RM maturity. These responses are analyzed in the next chapter.

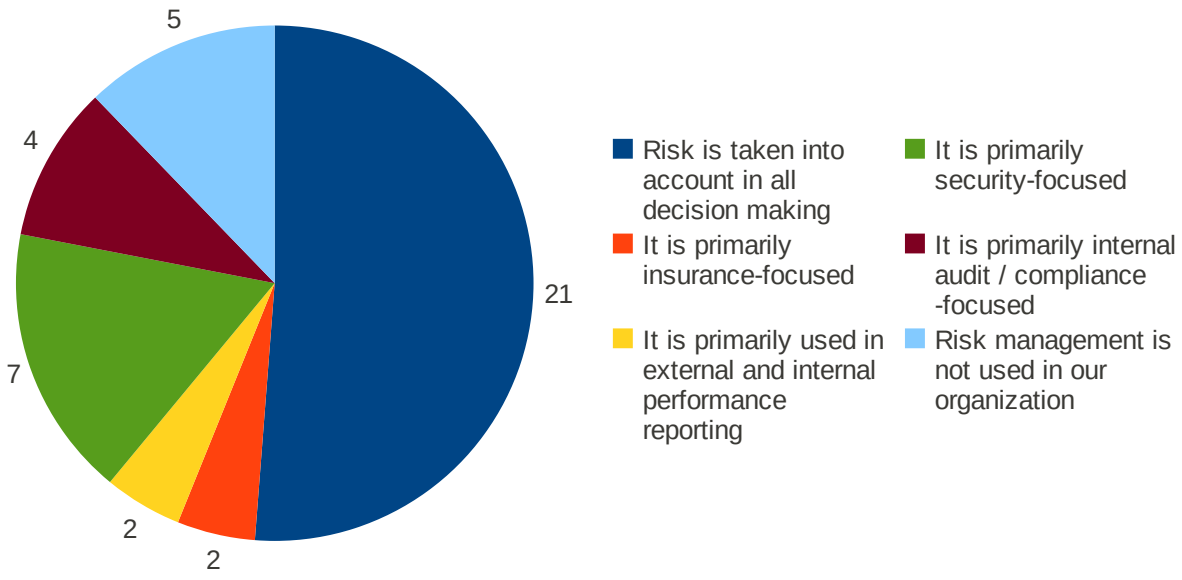


Illustration 14: B11: "How is risk management used within your organization?" n = 41

5.1 Risk Management Maturity Levels

In this chapter, the RM maturity is analyzed by average scores from the Likert scale questions. Scores greater than 4 were considered as a sign of high risk management maturity. Correspondingly, the threshold for low maturity was score value 2.

Firstly, in this chapter the RM maturity levels for all respondents are presented. The average maturity scores are examined per questions and per respondents. The respondents' maturity was measured by calculating the average of all their responses. By examining the average of the scores of respondents, disparities in RM maturity between large enterprises and SMEs can be identified. Correspondingly, the analysis of the maturity levels of individual questions reveals the weakest areas of RM. The maturity levels of the individual questions were measured by calculating the average of all responses submitted to the particular question. Consequently, the attention is turned to the questions indicating low RM maturity. By identifying the most problematic areas, this paper can contribute to the development of organizations' risk management.

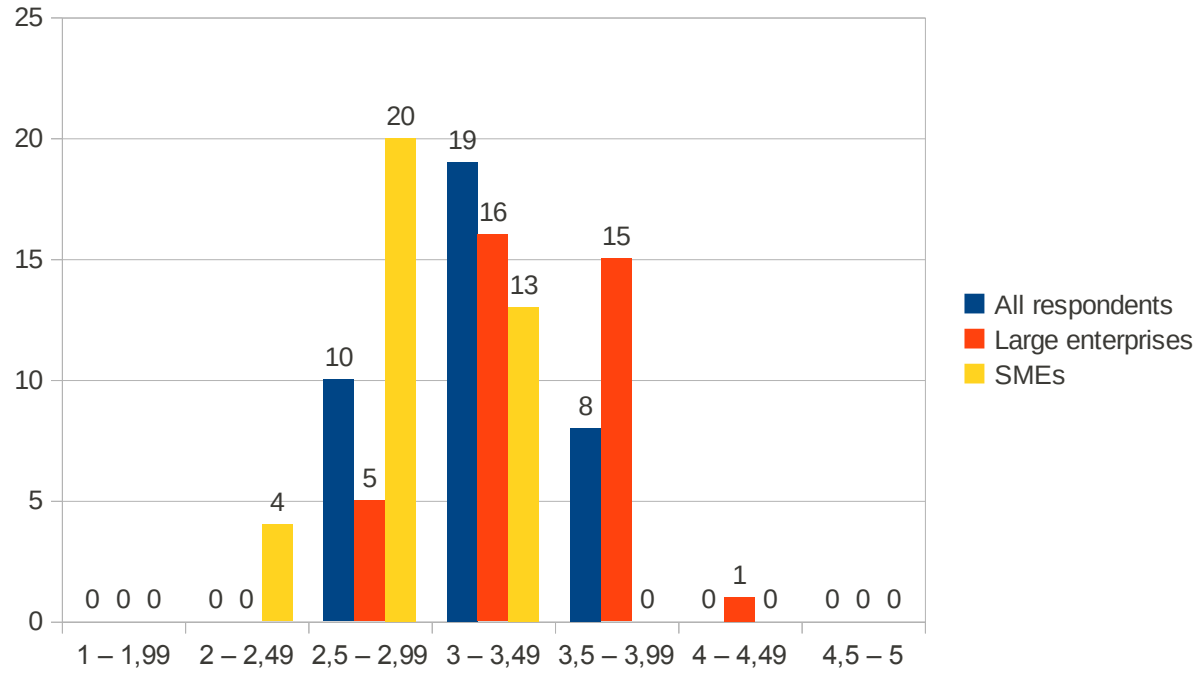


Illustration 15: Number of questions within each average score range, n = 37

The examination of the scores of *all respondents* reveals that the majority of the questions received an average grade slightly above the middle value 3. For the remainder of the questions (10/37), the average score was below the middle value. Surprisingly, none of the questions attracted responses with scores higher than 4 or lower than 2.

Table 1: Average scores per question

THEME	QUESTIONS						
Decision Making	Q1	Q2	Q3	Q4	Q5	Q6	
	3.21	3.33	3.67	3.07	3.07	3.19	
Commitment of management	Q7	Q8	Q9	Q10			
	3.55	3.62	3.26	3.38			
RMP	Q11	Q12	Q13	Q14	Q15	Q16	
	3.50	3.24	3.24	3.33	2.83	3.19	
Changes in operational environment	Q17	Q18					
	3.34	3.15					
Competences and accountabilities	Q19	Q20	Q21				
	3.07	2.86	2.98				
Information flows	Q22	Q23	Q24	Q25	Q26	Q27	
	3.60	3.75	2.86	2.73	3.50	3.21	
	Q28	Q29	Q30	Q31	Q32	Q33	
	3.17	2.95	3.02	3.00	3.12	2.93	
Performance measurement and continual improvement	Q34	Q35	Q36	Q37			
	2.78	2.59	2.70	3.50			

The Table 1 presents the average scores for each question. The questions and their abbreviations are presented verbatim in the Appendix 1. The average scores of all respondents ranged from 2.59 to 3.75. Comparing the responses of the *large enterprises* with the *SMEs* clearly shows that large enterprises are much better off with their risk management than the SMEs. Out of 37 Likert scale questions responded by the large enterprises, 32 questions had an average score greater than 3, whereas only approximately a third (13/37) of the questions responded by SMEs showed RM maturity above the middle value. With the SMEs, more than a half (24/37) of the questions fell into the category between 2 and 2,99. By comparison, a minuscule proportion (5/37) of the questions of the large enterprises had an average score of smaller than 3.

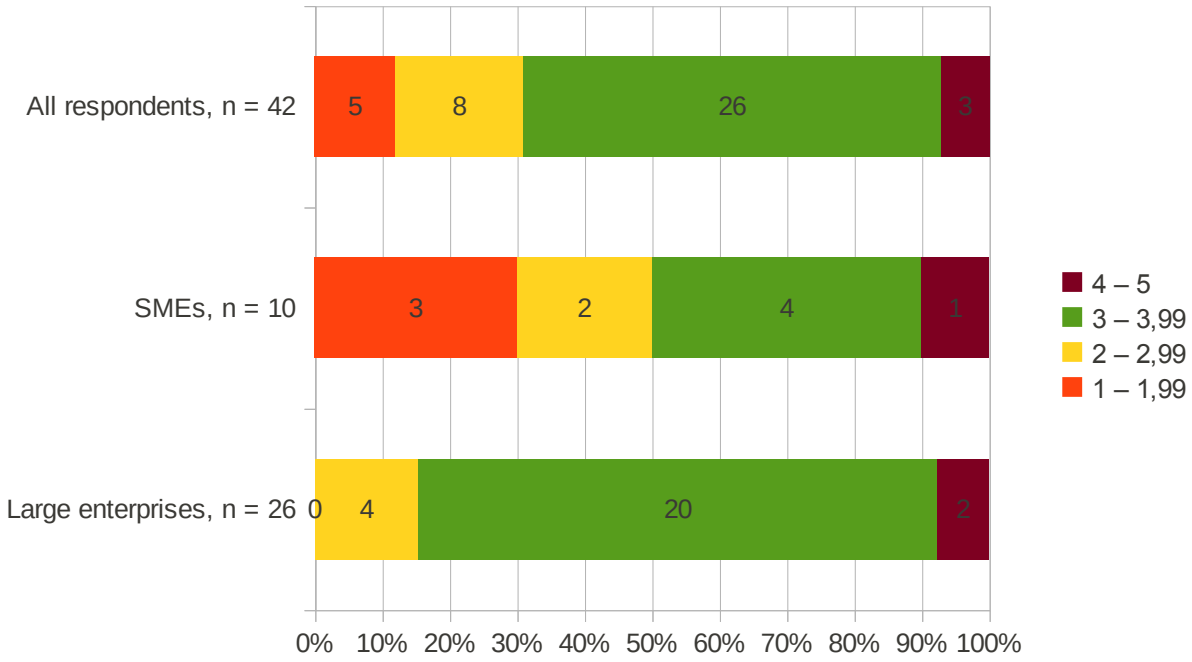


Illustration 16: Relative proportion of respondents with according average score

In the Illustration 16 above, the respondents are classified in score ranges depending on the average of all their 37 responses. The average scores are arranged in four interval ranges as indicated by the Illustration. The remaining six respondents that are not included in either large enterprises or SMEs are not considered separately, since they do not form a meaningful mutual category. These six respondents constitute of those organizations that do not have an annual turnover, such as public sector organizations, or have chosen not to express it.

Examination of the scores per respondent also reveals that the large enterprises were overall more successful in their risk management than small- and medium -sized ones. The vast majority (22 / 26) of the large enterprises had the average score of 3 or greater. Enterprises with high maturity were equally few in numbers in case of both SMEs (1/10) and large enterprises (2/26). Correspondingly, with almost a third of all the SMEs having a maturity score lower than 2, the results suggested that a significantly larger proportion of SMEs were low maturity organizations.

Table 2 lists these questions beginning from the lowest average score. In the table below, the averages of large enterprises and SMEs are compared to the average of all responses.

Table 2: The lowest performance scores (all respondents) and the corresponding results of large enterprises and SMEs

NUMBER OF QUESTION	ALL RESPONDENTS	LARGE ENTERPRISES	SMEs	QUESTION
Q35	2,58	2,72	2,4	Performance metrics currently in use depict realistically the performance of risk management.
Q36	2,7	2,76	2,89	Relevance of the performance metrics is regularly evaluated.
Q25	2,73	2,81	2,44	Information flows smoothly to your organization's external stakeholders.
Q34	2,78	2,88	2,8	Risk management performance is monitored regularly.
Q15	2,83	3,08	2,4	The interconnectedness of different risks is taken into account in decision making.
Q20	2,86	3,12	2,6	Employees have sufficient resources to assess risks.
Q24	2,86	2,88	2,8	Information flows smoothly to your organization's employees.
Q33	2,92	3,23	2,56	Risk register is up-to-date and supports decision making.
Q29	2,95	3,12	3	Risk management vocabulary is uniform in the whole organization.
Q21	2,97	3,23	2,7	Competence in your organization is used widely in assessing risks.

The results suggest that the performance measurement is a major area in need of improvement. The lowest score (2,58) was given to the realistic depiction of RM performance (Q35), with the regular performance measurement (Q34) and the regular re-evaluation of performance metrics (Q36) also among the weakest scores.

The inadequateness of information flows became apparent when considering the communication with the employees (non-managers) (Q24) and external stakeholders (Q25). For comparison, the information flows to those accountable for the direction and oversight of the organization were considered significantly more successful, with according scores 3,6 to the board of directors (Q22) and 3,75 to the senior management (Q23).

The risk management process is hindered by the lack of ability to recognize the interconnectedness of different risks (Q15). Moreover, the respondents evaluated that in assessing risks, the different areas of expertise in their organization were not fully utilized (Q21). Interestingly, the use of the external stakeholders' competence with regard to RMP (Q31) was considered of almost equally low-performing (average score 3.0).

Several deficiencies were also found in the framework supporting the management of risk. Employees seemed to to be insufficiently resourced (Q20) to assess risks. However, this result may be reflected in other questions, depending on the respondent's understanding of what is meant by "resourcing". "Resourcing" can be understood e.g. as time or available tools, including the risk registers (Q33). Part of the problems was the lack of a uniform vocabulary (Q29).

5.2 Discussion

The aim of this study was to investigate the ISO 31000 -compliance of Finnish organizations. The degree of compliance with the standard would serve as an indicator of RM maturity, or in other words, how successful risk management is currently in Finnish organizations. Since ISO 31000 is intended to be applicable to organizations of all sizes and industries, there are no uniform qualifications for how to implement the standard. The intention of the standard is to serve as a best-practice reference for certain elements that should be present in the risk management architecture. To assess the compliance with ISO 31000, this study used a series of self-evaluation questions with Likert scale approximations. The emphases of the standard formed the basis for the questionnaire, which is merely one interpretation of how to conduct an assessment on the compliance with ISO 31000. The open-ended questions were intended to enrich the data accumulated through the Likert scale questions.

In this chapter, the most remarkable findings of this study are discussed. Chapter 0 presented those areas of risk management with the average maturity scores lower than the threshold value 3. However, all of these areas are not brought to further examination. As revealed by the Table 2, majority of the average scores are very close to the middle value. Due to the relatively small amount of responses, even a few additional responses would have had a significant impact on the average scores. Therefore, rather than conducting an in-depth analysis of the individual questions,

a more meaningful approach is to examine the patterns emerging from the research data. Indeed, a few clearly visible designs were identified, including:

1. No area of risk management stood out in terms of exceptionally poor or great performance;
2. Large enterprises are more successful in their risk management than SMEs;
3. RM performance management constitutes a challenge for RM practitioners; and
4. The information flows to the board and senior management are more successful than the information flows to the employees and the external stakeholders.

The average score of every question was located in the range from 2 to 4. Thus, no single area of RM could be identified as having exceptionally low or high maturity. However, clear differences could be seen especially in terms of information flows. The surveys using the Likert scale approximations tend to suffer from the *central tendency bias*, in which the respondents, often due to indecision, tend to choose the middle value of the scale (Klos 2012). As the examination of the average scores suggests, the central tendency bias may have taken effect in this study as well.

The examination of the average scores revealed that SMEs tended to be worse off with their risk management when compared to large enterprises. This outcome seems logical when considering the assumption that smaller enterprises have typically fewer resources available, whether it be time, employee competence or monetary assets. These intuitive presumptions are substantiated by the univocal results gained in this study. The source of the problem herein may be the low awareness about the importance of RM. A recent study on the Finnish SMEs suggests that SMEs are typically motivated to RM by customers' requirements, business continuance and change management (Kupi, Keränen & Lanne 2009).

This study indicated that the RM practitioners face challenges with the performance measurement. Finding the right things to measure seems to be an insurmountable challenge. Weakness in performance management was also recorded in a recent survey by RIMS (2011), where more than a half of all the respondents described their performance management maturity as "ad hoc or non-existent" or "initial". Based on the responses to the open-ended questions, the

performance of RM is difficult to distinguish from the (1) overall performance of the organization and the (2) macroeconomic fluctuations. One respondent noted that *"...the outcome [of RM] is linked to other activities, which makes it hard to evaluate the performance as separate."* ISO 31000 suggests that RM performance should be measured by progress according the risk treatment plan (ISO 31000:2009, 20). The achievement of objectives, as stated by ISO 31000, is ultimately the measure that reveals whether RM is value-adding. As simple as this approach may seem, the truth is much more complicated. Whether the objectives are achieved will not only depend on the organization, but in many cases, external factors beyond the control and anticipation of the organization. How to take into account the impact of these random events when deciding how well the current risk management framework serves the needs of the organization is supposedly problematic.

Another cause for the problems with the performance measurement may lie in the overall confusion regarding what risk management actually is. As reflected by the open answers, the risk managers face challenges regarding the shared understanding on risk management inside the organization. As one respondent noted: *"Elements of RM are included in some important decisions, but people do not perceive that they are assessing risks or at least it is not called with that name."* Decision makers may not be aware that the decision making procedures and tools they are using are actually risk management. This problem is also partly reflected by the poor performance regarding the consistent and uniform use of RM vocabulary (Q29). Shared understanding on the basic terminological concepts and their meanings has been one fundamental intention of many RM standards, including ISO 31000. Substantiating the similar findings in the earlier studies (e.g. Kupi, Keränen & Lanne 2009), this study indicates that there is still work to be done with regard to achieving this target.

The responses indicated that information flows smoothly to the management and the board, whereas the employees and the external stakeholders were clearly worse off regarding this aspect. Nonetheless, this problem is a widely recognized one in management sciences. Thus, the communication deficiencies are not exclusively a hindrance for the risk management domain.One explanation for the difference of maturity is that the responses may possibly simply reflect communication *priorities*. Ensuring the information flows to the strategic-level decision makers

is typically perceived as more important than communication targeted to the employees and various stakeholders. One respondent remarked that a contemporary ICT-architecture facilitates plentiful availability of data, but this does not ensure *per se* that the risks are systematically discussed and processed at the senior level.

In ISO 31000, establishing effective communication and consultation mechanisms with all the relevant stakeholders is recognized as a key function of RM framework. For enterprises, the operational environment has been shifting during the recent years towards more complex networks, where it is no longer meaningful to examine enterprises merely as single legal entities, but as parts of a functional value network. Therefore, the deficiencies in the area of information flows may be a partial cause for the overall immaturity and lack of integration, which became apparent in the open answers. The opinion introduced in many open answers was that the intra-organizational understanding about RM was too diverse and too limited.

5.3 Limitations of the Study

As stated above, the total amount of responses (42) is satisfactory, although a larger number of responses would have added credibility and weight to the results. The comparison between the results of the large enterprises and the SMEs would have required a greater number of respondents representing the latter. The questionnaire was able to attract a mere 10 responses from SMEs, compared to 27 responses from large enterprises. Also, as stated earlier, the comparisons using other background factors, such as the use of RM standards and the industry, were thwarted by the minuscule amount of responses.

Without random sampling, the results of this study do not have statistical representativeness (e.g. Fowler 2002, 15). Therefore, the outcome can be regarded merely as directional. Furthermore, the large enterprises were disproportionately represented regarding their share of the total number of enterprises. Therefore, the results of this study are hardly to be generalized to the whole population of the enterprises. Since the large enterprises were found to be more mature in their RM, the average scores of all respondents are upwards biased.

The upwards bias may have been enhanced by yet another factor: the professional status of the respondents. As stated above in the Chapter 4, the responses were gathered via professional

sources dedicated to risk management -related fields. By this, it can be estimated that also a vast majority of the respondents were risk management professionals. It is likely that if an organization employs a risk management specialist, it also has a stronger dedication to risk management and higher RM maturity than an organization without a risk management specialist. Therefore, it can be concluded that the results show a somewhat higher maturity than an equivalent study would have revealed if conducted to a random sample of organizations. On the other hand, as discussed earlier in chapter 5.3, the central tendency bias may have affected the results as well.

As stated earlier in chapter 4, the questionnaire did not use quantitative proxies to measure RM maturity. On contrary, to respond the questions required a qualitative assessment of the particular area. Qualitative assessments such as the ones required in this survey always include a certain amount of vagueness and subjectivity, which may have distracted the respondents. Another further distracting factor is the formulation of the questions, which included ambiguous terms such as "holistic". Although an ideal question is identically understood by every respondent, the questions, to some extent, are subject to subjective understanding. This problem is further aggravated by the diversity of the risk management terminology with the lack of shared understanding on key definitions.

6 CONCLUSIONS

The requirements for effective risk management have grown during the recent years. The first decade of the current millennium has seen a number of economic crises, beginning from the collapse of Enron in 2001 to the latest capital market crisis in 2008, which have been drivers for increased corporate governance. The globally interconnected economy calls for heightened awareness of the uncertainty factors related to the operational environment.

As a response to these emerging needs, a substantial growth and development has been seen in the risk management industry. However, the diversity of different actors in the playing field has been a source for much confusion and ambiguity with regard to mutual RM practices and the use of terminology. The attempts to harmonize risk management practices have been actualized in a number of risk management standards. Despite the failures of the earlier standards to achieve the status as the worldwide top benchmark for risk management practices, great expectations have been placed on ISO 31000. The early results gained in this study and the few other ones mapping the usage of the new standard (G31000 2012; RIMS 2011) have been promising.

In spite of the widespread interest towards the standard, the results of this study imply that the current best practice risk management as presented in ISO 31000 is not yet reality among the Finnish organizations. Especially the small- and medium-sized enterprises are lacking of good RM practices. Furthermore, whereas ISO 31000 emphasizes communication with all stakeholder groups, the communication priorities within the respondents are increasingly emphasized on the top decision makers in the organization.

Due to the very recent date of publication, ISO 31000 is still an uncharted territory in the academia. As noticed, only a few academic research reports have contributed to the newly published standard, thus leaving plenty of space for a plethora of new studies. The impact of the use of ISO 31000 on the risk management performance is still an open issue. An attempt to address that issue was made in the context of this study, but unluckily, the pursuit was thwarted by the small amount of responses. Implementation of the standard is to be examined in the new

implementation guide ISO 31004, which is scheduled to be published in 2014. This will undoubtedly reveal many of the open questions related to the implementation.

Survey studies such as the present one are always subject to certain amount of indeterminacy regarding their inherent potency to portray the examined phenomenon. Fundamentally, the picture about the reality is drawn by the more or less subjective perceptions of the respondent. Furthermore, the research is further complicated by the survey questions, which lay yet another layer of interpretation between the "truth" and the researcher. These flaws need to be taken into account when examining the results of this survey. Another puzzling factor regarding this study is the relatively small total amount of responses. However, despite the limitations of this study, it is to be believed that its results will prove to benefit the scientific community and risk management practitioners. If ISO 31000 will gain its position as a global, best-practice risk management standard, as anticipated, the knowledge of its application will prove to be useful.

7 REFERENCES

7.1 Literature

Alasuutari, Pertti. 1998. An invitation to social research. Sage, London.

Bernstein, Peter L. 1996. Against the Gods - The Remarkable Story of Risk. John Wiley & Sons, Inc. New York.

Cooper, Donald R. & Schindler, Pamela S. 2003. Business Research Methods. 8th ed. Boston, MA: McGraw-Hill Irwin, cop.

Crouhy, Michel; Galai, Dan & Mark, Robert. 2005. Essentials of Risk Management. Blacklick, OH: McGraw-Hill Professional Publishing.

Fowler, Floyd J. Jr. 2002. Survey Research Methods. 3rd ed. Thousand Oaks : Sage, cop.

Hillson, David. 2010. Exploiting Future Uncertainty: Creating Value from Risk. Farnham, Surrey, GBR: Ashgate Publishing Group.

Hirsjärvi, Sirkka & Remes, Pirkko & Sajavaara, Paula. 2007. Tutki ja kirjoita [in English: Research and write]. 13th ed. Helsinki: Tammi.

Kamppinen, Matti & Raivola, Petri & Jokinen, Pekka & Karlsson, Hasse. 1995. Riskit yhteiskunnassa: Maallikot ja asiantuntijat päätösten tekijöinä [in English: Risks in society: Laymen and experts as decision makers]. 2nd ed. Helsinki: Gaudeamus.

Kloman, H. Felix. 2008. Fantods of Risk. Lyme, CO: Seawrack Press Inc.

Laurila, Pentti.J. 1981. Riskienhallinta [in English: “Risk Management”]. Vakuutusalan kustannus. Helsinki.

Longman. 2003. Dictionary of Contemporary English. Harlow, ENG: Pearson Education Ltd.

Pritchard, J.A.T, 1978. Risk Management in Action. NCC. Manchester.

Rubin, Robert J. & Rubin, Irene S. 2005. Qualitative interviewing : the art of hearing data. 2nd ed. Thousand Oaks: Sage, cop.

Saunders, Mark & Lewis, Philip & Thornhill, Adrian. 2009. Research methods for business students. 5th ed. Harlow: Prentice Hall, cop.

Silverman, David. 2005. Doing Qualitative Research. 2nd ed. London: Sage

Suominen, Arto. 2003. Riskienhallinta [in English: “Risk Management”]. 3rd ed. Helsinki: WSOY.

Vaughan, Emmett & Vaughan, Therese. 2001. Essentials of Risk Management and Insurance. 2nd ed. New York, NY: John Wiley & Sons.

7.2 Articles in Compilations

Aabo, Tom & Fraser, John R.S. & Simkins, Betty, J. 2010. The Rise and Evolution of Chief Risk Officer - Enterprise Risk Management at Hydro One. In: Fraser, John R.S. & Simkins, Betty J. [ed.]. Enterprise Risk Management. Hoboken, New Jersey: John Wiley & Sons, Inc. 531 - 556.

Ale, B., Aven, T. & Jongejan, R. 2010. Review and discussion of basic concepts and principles

in integrated risk management. In: Guedes Soares, C., Bri, Radim & Martorell, Sebastián [ed.]. Reliability, Risk, and Safety, Theory and Applications, ESREL 2010. London: CRC Press. 421 - 427.

Branson, Bruce C. 2010. The Role of the Board of Directors and Senior Management in Enterprise Risk Management. In: Fraser, John R.S. & Simkins, Betty J. [ed.]. Enterprise Risk Management. Hoboken, New Jersey: John Wiley & Sons, Inc. 51 - 67.

Carroll, Terry. 2010. A Holistic Approach To Business Risk Management. In: Abkowitz, Mark & Beretz, Paul & Chambers, Andrew [ed.]. Approaches to Enterprise Risk Management. Huntingdon, GBR: Bloomsbury Information Ltd. 9 - 12.

Henriksen, Per & Uhlenfeldt, Thomas. 2006. Contemporary Enterprise-Wide Risk Management Frameworks. In: Andersen, Torben Juul [ed.]. Perspectives on Strategic Risk Management. Gylling: Copenhagen Business School Press. 107 - 129.

Iyer, Subramanian R. & Rogers, Daniel A. & Simkins, Betty J. 2010. In: Fraser, John R.S. & Simkins, Betty J. [ed.]. Enterprise Risk Management. Hoboken, New Jersey: John Wiley & Sons, Inc. 419 - 439.

Kloman, Felix H. 2010. A Brief History of Risk Management. In: Fraser, John R.S. & Simkins, Betty J. [ed.]. Enterprise Risk Management. Hoboken, New Jersey: John Wiley & Sons, Inc. 19 - 29.

Mikes, Anette. 2010. Becoming the Lamp Bearer: The Emerging Roles of the Chief Risk Officer. In: Fraser, John R.S. & Simkins, Betty J. [ed.]. Enterprise Risk Management. Hoboken, New Jersey: John Wiley & Sons, Inc. 71 - 85.

Schrøder, Peter W. 2006. Impediments to Effective Risk Management. In: Andersen, Torben Juul [ed.]. Perspectives on Strategic Risk Management. Gylling: Copenhagen Business School Press. 65 - 88.

Shortreed, John. 2010. ERM Frameworks. In: Fraser, John R.S. & Simkins, Betty J. [ed.]. Enterprise Risk Management. Hoboken, New Jersey: John Wiley & Sons, Inc. 97 - 123.

7.3 Risk Management Standards

Committee of Sponsoring Organizations of the Treadway Commission (COSO). 2004. Enterprise Risk Management - Integrated Framework: Executive Summary & Framework. Jersey City, NJ: COSO.

DeLoach, James W. 2000. Enterprise-die Risk Management: Strategies for Linking Risk and Opportunity. London: Financial Times Prentice Hall.

Federation of European Risk Management Associations (FERMA). 2003. A Risk Management Standard. http://www.ferma.eu/wp-content/uploads/2011/11/a-risk-management-standard-english-version.pdf (Accessed 28.1.2012)

Institute of Internal Auditors (IIA). 2010. International Standards for the Professional Practice of Internal Auditing.(15.11.2011) http://www.theiia.org/download.cfm?file=35336

IRM / AIRMIC / ALARM. 2002. Risk Management Standard. London: IRM / AIRMIC / ALARM.

ISO. 2009. ISO Guide 73:2009 - Risk Management - Vocabulary. Geneva: ISO.

ISO. 2009. ISO 31000: 2009 - Principles and Guidelines on Implementation. Geneva: ISO.

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

RIMS. 2006. Risk Maturity Model (RMM) for Enterprise Risk Management.

Standards Australia and Standards New Zealand. 2004. Risk management: AS/NZS 4360:2004. Sydney: Standards Australia International.

7.4 Research Reports

Accenture. 2011. Global Risk Management Study.

Al-Darwish, Ahmed & Hafeman, Michael & Impavido, Gregorio & Kemp, Malcolm & O'Malley, Padraic. 2011. Possible unintended consequences of Basel III and Solvency II. IMF Working paper, WP/11/87.

Aon. 2010. Global Enterprise Risk Management Survey 2010. Chicago: AON Corporation.

Aven, Terje. 2011.On the new ISO guide on risk management terminology. Reliability Engineering & System Safety (2011). Vol. 96, No 7, July 2011. 719-726.

Beasley, Mark S. & Clune, Richard & Hermanson, Dana R. 2005. Enterprise riskmanagement: An empirical analysis of factors associated with the extent of implementation. Journal of Accounting and Public Policy. Volume 24, Issue 6, November–December 2005, 521–531.

Corporate Executive Board. 2008. Risk Management Effectiveness Survey Findings.

COSO. 2010. Report on ERM.

Deloitte. 2011. Global risk management survey, seventh edition - Navigating in a changed world.

G13000. Global ISO 31000 Survey 2011 - Results and Analysis. 2012.

Hills, M.W. 2011. Mass Gatherings and the Application of the New International Risk Management Standard ISO 31000. Prehospital and Disaster Medicine, Vol. 26. s75-s75.

Kamiya, Shinichi & Shi, Peng & Schmit, Joan & Rosenberg, Marjorie. 2007. Risk management terms. Working paper, March 2007.

Klos, Alexander. 2012. Central Tendency Bias and Self-Reported Risk Attitudes. Working paper.

Kupi, Eija & Keränen, Jaana & Lanne, Marinka. 2009. Riskienhallinta osana pk-yritysten strategista johtamista [in English: Integrating risk management into strategic planning in SMEs]. VTT.

Leitch, Matthew. 2010. ISO 31000:2009—The New International Standard on Risk Management. Risk Analysis, Vol. 30, No. 6. 887 - 892.

Liebenberg, André P. & Hoyt, Robert E. 2003. The Determinants of Enterprise Risk Management: Evidence From the Appointment of Chief Risk Officers. Risk Management and Insurance Review, Volume 6, Issue 1, February 2003, 37–52

Linsmeier, Thomas J. & Pearson, Neil D. 2000. Value at Risk. Financial Analysts Journal. Vol. 56, No. 2. 47-67.

Miller, Kent D.1992. A Framework For Integrated Risk Management In International Business. Journal of International Business Studies, Vol. 23, No. 2. 311 - 331.

Pagach, Donald & Warr, Richard. 2011. The Characteristics of Firms That Hire Chief Risk Officers. Journal of Risk and Insurance, Vol. 78, Issue 1, March 2011, pages 185–211.

Power, Michael. 2009. The risk management of nothing. Accounting, Organizations and Society, Vol. 34, 849-855.

PricewaterhouseCoopers (PwC). 2011. State of the internal audit profession survey - Territory report from Finland.

Purdy, Grant. 2010. ISO 31000:2009—Setting a New Standard for Risk Management. Risk Analysis, Vol. 30, Issue 6. 881 – 886.

Raz, Tzvi & Hillson, David. 2005. A Comparative Review of Risk Management Standards. Risk Management: An International Journal, 7(4). 53 - 66.

RIMS. 2011. Enterprise Risk Management Survey.

Slovic, Paul. 1987. Perception of risk. Science, Vol. 236. 280 – 285.

7.5 Other Sources

Arvopaperimarkkinayhdistys. 2010. Suomen listayhtiöiden hallinnointikoodi [in English: Corporate governance code for Finnish public companies].

Basel Committee on Banking Supervision. 2010. Consultative Document: Principles for Enhancing Corporate Governance. Basle, Switzerland: Bank for International Settlements (BIS).

Central Chamber of Commerce (CCC) Finland. 2006. Improving Corporate Governance of Unlisted Companies.

Everett, Catherine. 2011. A risky business: ISO 31000 and 27005 unwrapped. Computer Fraud & Security. February 2011. 5 - 7.

European Commission. 2003. Commission recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (2003/361/EC).

Lund, Mass S. & Solhaug, Bjørnar & Stølen, Ketil. 2010. Evolution in relation to trust and risk management. Computer. May 2010. 49 -55.

7.6 Internet Sources

ISO. About ISO. (13.2.2012a) http://www.iso.org/iso/about.htm

ISO. LinkedIn group carries out global survey of ISO 31000 - Deadline extended to 30 November 2011 (17.1.2012b) http://www.iso.org/iso/iso_catalogue/management_and_leadership_standards/risk_management.htm

ISO. New ISO/IEC standard on risk assessment complements risk management toolbox. (12.1.2012c) http://www.iso.org/iso/pressrelease.htm?refid=Ref1288

ISO. Technical Committee 262: ISO/AWI 31004. (15.11.2011d) http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=56610

Official Statistics of Finland (OSF). 2010. Finnish enterprises [e-publication]. Helsinki: Statistics Finland. (2.3.2012). <http://www.stat.fi/til/syr/2010/syr_2010_2011-11-25_tie_001_en.html>

SRHY. The Finnish Risk Management Association. (15.2.2012) http://srhy.fi/index.php?page=eng1

7.7 Interviews

Väisänen, Lassi (Consultant Entrepreneur and Executive Director, FinnRiMa). 11.11.2011. The digital recording (file type: .amr) on the interview is in the possession of the author.

8 APPENDICES

8.1 Appendix 1

Muista myös taulukoida miltä sivulta standardista!

THEME	**CODE**	IN ENGLISH	IN FINNISH
1. Background information	B1	What is the industry of your organization?	Mikä on organisaationne toimiala?
	B2	How many employees currently work in your organization?	Kuinka monta henkilöä organisaatiossanne tällä hetkellä työskentelee?
	B3	[enterprises] What is your annual turnover?	[yritykset] Mikä on yrityksenne liikevaihto
	B4	[enterprises] Is your company enlisted in Helsinki Stock Exchange?	[yritykset] Mikä on yrityksenne liikevaihto
	B5	What is your main area of responsibility?	Mikä on toimenkuvanne?
	B6	Respondent's work experience in current duties	Kuinka monen vuoden työkokemus teillä on nykyisiin työtehtäviinne tai vastaviin työtehtäviin liittyen?
2. Risk management standards	B7	Standards and frameworks currently in use	Mitä seuraavista standardeista / ohjeistuksista organisaationne käyttää?
	B8	How well are you acquainted with ISO 31000?	Kuinka hyvin tunnette riskienhallinnan standardin ISO 31000:2009?
	B9	Has your organization implemented ISO 31000?	Onko organisaationne implementoinut ISO 31000 -standardin?
3. Approach to risk management	B10	Which ones of the following statements best describe your organization's orientation to risk management?	Mikä seuraavista väittämistä parhaiten kuvaavat organisaationne suhtautumista riskienhallintaan?
	B11	How is RM used within your organization?	Kuinka riskienhallintaa hyödynnetään organisaatiossanne?
4. Decision making	Q1	Risks are taken into account in all decision making.	Kaikessa päätöksenteossa otetaan huomioon päätöksiin liittyvät riskit.
	Q2	RM creates clearly demonstrable value for your organization.	Riskienhallinta luo selkeästi osoitettavaa arvoa organisaatiollenne.
	Q3	Decision making aims at reaching organization's objectives.	Päätöksenteossa tavoitellaan organisaation tavoitteiden saavuttamista.
	Q4	Risks involved in potential alternatives is taken into account in decision making.	Päätöksenteossa huomioidaan mahdollisiin vaihtoehtoihin liittyvä riski.
	Q5	Consequences of different alternatives are taken holistically into account in decision making.	Eri vaihtoehtojen seuraukset huomioidaan päätöksenteossa kokonaisvaltaisesti.
	Q6	Stakeholders' opinions and perceptions are taken into account in decision making.	Päätöksenteossa otetaan huomioon sidosryhmien mielipiteet ja näkemykset.

5. Risk management and organization's management	Q7	The managers are committed to facilitating RM.	Organisaationne johtajat ovat sitoutuneet riskienhallinnan mahdollistamiseen.
	Q8	The board of directors is committed to facilitating RM.	Organisaationne hallitus on sitoutunut riskienhallinnan mahdollistamiseen.
	Q9	The managers understand the meaning of RM as a part of strategy execution.	Organisaationne johtajat ymmärtävät riskienhallinnan merkityksen osana strategian toteuttamista.
	Q10	The board of directors understand the meaning of RM as a part of strategy execution.	Organisaationne hallitus ymmärtää riskienhallinnan merkityksen osana strategian toteuttamista.
6. The RMP	Q11	The decision makers of your organization can identify and evaluate different alternatives and risks involved.	Organisaationne päätöksentekijät kykenevät identifioimaan ja arvioimaan eri vaihtoehtoja, sekä niihin kuuluvia riskejä.
	Q12	In assessing risks, the effect of consequences on the whole organization is taken into account.	Riskien arvioinnissa huomioidaan riskin seurausten vaikutus koko organisaatioon.
	Q13	In assessing risks, the effect of consequences on external stakeholders is taken into account.	Riskien arvioinnissa huomioidaan riskin seurausten vaikutus ulkoisiin sidosryhmiin.
	Q14	Risks are assessed with meaningful tools suitable for the particular situation.	Riskejä analysoidaan kuhunkin tilanteeseen sopivalla tavalla.
	Q15	The interconnectedness of different risks are taken into account in decision making.	Eri riskien väliset riippuvuudet huomioidaan päätöksenteossa.
	Q16	The criteria used in assessing the gravity of the risks are up-to-date.	Riskin vakavuuden arvioinnissa käytettävät kriteerit ovat ajankohtaisia.
	O1	In your organization, what are the major challenges regarding the risk assessment and treatment?	Mitkä ovat suurimmat riskien arviointiin ja hoitamiseen liityvät haasteet organisaatiossanne?
7. Changes in the operational environment	Q17	The impact of changes in operational environment on objectives is regularly monitored.	Toimintaympäristön muutoksien vaikutusta tavoitteisiin arvioidaan säännöllisesti.
	C1	How often are the changes in operational environment reported to the board?	Kuinka usein toimintaympäristön muutoksia raportoidaan hallitukselle?
	Q18	The information reported to the board is compact and relevant.	Hallitukselle raportoitava tieto toimintaympäristön muutoksista on riittävän tiivistä ja relevanttia.
8. Risk management competence	Q19	Employees are aware of the risks they are accountable for.	Työntekijät ovat tietoisia vastuullaan olevista riskeistä.
	Q20	Employees have sufficient resources to assess risks.	Työntekijöillä on riittävät resurssit riskien arvioimiseen.
	Q21	Competencce in your organization is used widely in assessing risks.	Organisaatiossanne olevaa osaamista hyödynnetään laajasti riskien arvioinnissa.
	O2	In your organization, what are the major challenges in RM competences?	Mitkä ovat organisaatiossanne suurimmat riskienhallinnanosaamiseen liittyvät haasteet?
9. Information flows		Information flows smoothly to your organization's...	Tieto liikkuu sujuvasti organisaation...
	Q22	...board of directors.	…hallitukselle.
	Q23	...senior management.	…johtoryhmälle.
	Q24	...employees.	…työntekijöille.

	Q25	...external stakeholders.	..ulkoisille sidosryhmille.
	Q26	Information reported to the board is sufficiently compact and relevant.	Hallitukselle raportoitava tieto on riittävän tiivistä ja relevanttia.
	Q27	Databases supporting decision making are conveniently available.	Organisaatiossanne päätöksenteon tukena olevat tietovarannot ovat helposti saatavilla.
	Q28	Databases supporting decision making are sufficient and up-to-date.	Organisaatiossanne päätöksenteon tukena olevat tietovarannot ovat riittäviä ja ajankohtaisia.
	Q29	Risk management vocabulary is uniform in the whole organization.	Riskienhallinnassa käytettävä sanasto on yhdenmukaista koko organisaatiossa.
	Q30	Your organization's communication is two-sided.	Organisaationne viestintä on kaksisuuntaista.
	Q31	Know-how of external stakeholders is utilized in risk assessment.	Ulkoisten sidosryhmien tietoa hyödynnetään riskienarvioinnissa.
	Q32	All decision making is documented and justified.	Kaikki päätöksenteko on perusteltua ja dokumentoitua.
	Q33	Risk register is up-to-date and supports decision making.	Riskirekisteri on ajantasainen ja päätöksentekoa tukeva.
	O3	What are the major communications-related challenges in your organization?	Mitkä ovat suurimmat viestintään liittyvät haasteet organisaatiossanne?
10. Performance measurement and continual improvement	Q34	Risk management performance is monitored regularly.	Riskienhallinnan suorituskykyä mitataan säännöllisesti.
	Q35	Performance metrics currently in use depict realistically the performance of risk management.	Käytettävät suorituskyvyn mittarit kuvaavat realistisesti riskienhallinnan suorituskykyä.
	Q36	Relevance of the performance metrics is regularly evaluated.	Suorituskyvyn mittareiden relevanssia arvioidaan säännöllisesti.
	Q37	In all operational development, the economic meaningfullness is taken into account.	Kaikessa kehittämistoiminnassa huomioidaan kehittämisen taloudellinen mielekkyys.
	O4	In your organization, what are the major challenges in development and performance measurement?	Mitkä ovat organisaatiossanne kehittämiseen ja suorituskyvyn mittaamiseen liittyvät suurimmat haasteet?