Concept for an internal ERM report

12. The Continuing Professional Development Program for Security Management

Project work

Jaana M Lappalainen

Metso Group

DIPOLI Congress Centre 2.4.2013

Aalto University Professional Development – Aalto PRO

Tiivistelmä

Tutkielman tavoitteena on löytää malli konsernitason riskienhallinnan tuottamalle sisäiselle riskiraportille luonnostelemalla riittävän hyvät käytännöt ylimmän johdon päätöksentekoa tukevalle raportille. ISO 31000 -standardi ja COSO:n kokonaisvaltainen riskienhallinta luovat pohjan tutkielmalle.

Tutkielma on laadittu tarkastelemalla olemassa olevia säädöksiä, suosituksia ja kirjallisuutta mukaan lukien tunnetuimpien ja käytetyimpien riskienhallinnan ja liiketoiminnan johtamisen raportointisuositukset.

Lakisääteiset ja vaatimustenmukaisuutta valvovat viranomaiset eivät ole asettaneet erityisiä sisäistä riskiraportointia koskevia vaatimuksia. Yleisesti käytetty lähestymistapa on arvioida kohderyhmien tiedon tarpeita. Yleispätevän kaikille sopivan raporttimallin sijasta eri kohderyhmät jopa yhtiön sisällä tarvitsevat eritasoista tietoa.

Ihanteellinen hallitustason riskiraportti koostuu riskienhallinnan suorituksen, lyhyen ja pitkän aikavälin uhkiin ja mahdollisuuksiin, kriittisiin uhkiin, kehittyviin riskeihin sekä riskien käsittelyyn liittyvistä tiedoista. Johtoryhmän raportti voi sisältää konkreettisempia yksityiskohtia riskeistä mukaan lukien tiedot seurannasta, riskien käsittelystrategiasta ja merkittävimpien riskien vastuuhenkilöistä.

Sisältö-, rakenne- ja taajuussuositusten lisäksi tutkielmassa hahmotellaan raportoinnin viitekehyksen pääelementit sekä riskiraportin sisäiset kriteerit.

Abstract

The target of the project work is to find a concept for the internal risk report prepared by a corporate-level risk management function and to outline good-enough practices for the report to support top management's decision making. The ISO 31000 standard and the COSO ERM framework form a basis for the project.

The project is carried out by reviewing existing regulations, recommendations and related literature, including an overall review of the most well-known and widely used risk and business management reporting recommendations.

There are no specific requirements for internal risk reporting set by statutory or compliance authorities. A commonly used approach is to evaluate the information needs of the target groups. Instead of a generic, one-fit-for-all report concept, different target groups – even within a single company – need different levels of information.

An ideal board-level risk report consists of information on risk management performance, short- and long-term threats and opportunities, critical threats, emerging risks and a risk treatment overview. An executive management report can include more tangible details of risks, including monitoring, treatment strategies and assignment of accountabilities for key risks.

Besides the content, structure and frequency recommendations, the project work outlines the key elements of an internal risk report framework and defines internal criteria for the risk report.

Contents

1 Introduction

Today's global business and competitive environment is increasingly complicated and subject to a wide range of risks, because of the complexity, interdependence and uncertainty of the world we live in. Accumulation risks are growing in complexity and have implications on risk management and business development. Accordingly, the company is put under more pressure to protect and sustainably optimize shareholder value. In this context, the company's internal and external stakeholders require in-depth information on opportunities (upside risks) and threats (downside risks), and how the company responds to risks.

The role of risk management is to support the achievement of the company's strategic targets and business objectives and the continuity of operations. Risk management provides support for strategic and operative decision making and planning, improves the agility needed to take advantage of, minimize, remove or mitigate risks and increases general stakeholder confidence.

Despite the fact that risk management is generally – or at least it should be – included in management's daily decision making regarding operational activities, strategic planning and implementation, investments, specific projects and business continuity plans, there is still an internal order for consolidated overall risk information at the board level as well.

Risk management functions must find a balance between what to select from the vast amount of risk information and what "in-depth risk information" the key internal stakeholders want/need to have. As a risk management expert, the function should be able to identify the most essential issues that top management needs to be aware of from the vast amount of risk data.

As a fundamental part of the risk management process, risk and risk management reporting is also an essential part of management reporting – even if it is done in a separate report and at a different frequency than the management reports.

Recommendations of the well-known risk management frameworks and standards, such as the COSO ERM and the ISO 31000 standard, emphasize that companies should report on their risks and risk management. Listed companies have to comply with various statutory and compliance obligations regarding risk information to satisfy the mandatory regulatory external disclosure requirements and internal control.

Based on the ISO 31000 risk management standard (2009, p.1), risk is the effect of uncertainty on objectives. Being an uncertainty factor of the future, it is strongly connected to a company's strategy implementation. While assessing future threats and opportunities, a company seeks to evaluate factors that may endanger or enhance the future success of the company: risk is either an opportunity for benefit or a threat to success, or a combination of both aspects. What are these uncertainty factors of the future related to strategy implementation, and how does a company respond to them remain the two most essential questions in outlining the content for a systematic internal risk reporting concept.

The study reviews the development of the risk reporting concept of a corporate risk management function in accordance with regulatory requirements, recommendations etc. requirements. The study focus is on the internal risk reporting requirements of a risk management function that complies with the enterprise risk management framework, conducts risk assessments and risk governance evaluations, is responsible for overall coordination of corporate security elements and administration of insurance programs, but which does not operatively manage risks. The challenge is to define which of the risk management function's responsibility areas should be systematically reported internally and how often, and what is the most appropriate reporting format. The core is to study if there are any specific guidelines regarding risk reporting, and especially internal risk reporting.

Due to the fact that standards, frameworks and guidelines tend to be conceptual with little guidance on practical implementation, the study includes an

overall review of the most well-known and widely used risk management organizations and management strategic partners' risk report recommendations.

The target of the study is to draft an ideal concept (i.e. content and practices) for a company's internal risk report based on recommendations, suggestions and identified information needs. Content requirements are limited to issues within the scope of responsibility of a corporate-level risk management function. Legislation related to accounting and financial reporting and to occupational safety and health is left out of the scope. Stakeholders are limited to internal stakeholders.

The study first concentrates on risk reporting and on what it means as well as what kinds of attributes are associated with it. Since the assumption is that internal risk reporting, let alone the internal risk report, is not covered in regulations, standards or guidelines related to listed company risk reporting, the project work has been started by studying external risk reporting guidelines to find any indications that could be applied internally to risk reporting and the internal risk report.

The study is divided into three phases:

1. Review of existing laws, regulations, governance statements and related literature

2. Consolidation and evaluation of the key findings derived from the review

3. Outlining of a concept for the internal risk report based on the key findings

The first step of the study, after the basic terminology definition, is to determine what is meant by "risk reporting and risk report." Do the COSO ERM framework or ISO 31000 standard give any definitions, guidelines or recommendations? Does any legislation, regulation, national, European or global organizational level corporate governance, stock exchange or national financial market supervisor, major insurance and management consulting company, or risk management literature give any definitions, guidelines or recommendations? This is done by simply by executing a literature overview.

The second step is to compile a summary of the most relevant risk report elements based on the literature review.

The final step is to outline a draft of an ideal risk report concept based on the above key findings and on the writer's own experiences, including definitions regarding the report's content, structure, format and frequency.

It should be noted that this study is not done for any specific company, but for any company that is interested in developing its internal risk report.

2 Background to the study

The target of the study is to find a concept model for the internal risk and risk management report delivered by a corporate-level risk management function. The aim is to outline good-enough practices for the internal risk reporting to support top management's decision making. The assumption that the ISO 31000 standard and the COSO ERM framework are the starting points and thus form a basis for the entire concept. To support the formal reporting concept approach, statutory and governance regulations are used to enhance the risk report concept. In addition, a small sample of risk management literature is used as a source of background information.

The external risk report is left out of the scope, to keep the study within the given framework. Besides, listed companies – especially in Finland – are very compliant with existing laws and regulations related to the external disclosure of risk information. Nevertheless, external risk reporting requirements are reviewed in order to find possible development ideas for internal risk reporting and internal risk reports.

The purely financial accounting requirements related to risks are beyond the scope in this study simply because financial accounting is not the responsibility of the corporate risk management function. The study focuses on guidelines aimed directly at issues for which corporate risk management is responsible in one way or another.

In addition to limiting the study to the application of internal reporting, the internal target groups are narrowed into two organizational decision-making bodies: the board of directors and the executive management. The board is responsible for strategic decisions and the executive management for the strategy implementation. The target groups require different levels of risk information (from overall to detailed) in order to utilize the information in their respective decision-making processes. The board-level commitment to

risk management is critical for successful decision making and for value driving.

Figure 1 The image illustrates the content elements of the risk report concept framework

2.1 Basic definitions of risk, risk management and risk reporting

Before going into detail, it is useful to have a look at the basic terminology related to risk, risk management and risk reporting.

Risk is defined as an effect of uncertainty on objectives. It can have different aspects, such as financial, health and safety, and environmental, and it can apply at different levels, such as strategic, organization-wide, project, product, and process. An effect may be positive, negative or a deviation from the expected, and that risk is often described by an event, a change in circumstances or a consequence. (ISO/IEC Guide 73:2009, p. 1-2)

According to the ISO/IEC Guide 73 (2009, p. 2), risk management refers to coordinated activities to direct and control an organization with regard to risk. Enterprise risk management is a process designed to identify potential events that may affect a company to provide reasonable assurance regarding the achievement of entity objectives (COSO 2004, p. 2).

Risk reporting is defined as a form of communication intended to inform particular internal or external stakeholders by providing information regard-

ing the current state of risk and its management (ISO/IEC Guide 73:2009, p. 12).

In short, risk reporting is a process to inform stakeholders on issues related to risks and risk management. According to Ilmonen et al. (2010, p. 193), the target of risk reporting is to increase the awareness and transparency of risks and improve the operational efficiency and value creation.

Franks (2007) underlines that risk reporting should demonstrate that an organization is managing its key risks. But more importantly, it should also show whether there are risks that can be exploited for growth. A lot risk reporting tends to be all about the down-side. (see Fagg 2007)

PwC sees risk reporting from the risk evaluation perspective. The purpose of a risk report is to facilitate risk monitoring by providing necessary information and analysis of the existing and potential risks to which the company is exposed (PwC 2012, p. 42).

In this context, a stakeholder is a person or an organization than can affect, be affected by, or perceive themselves to be affected by a decision or activity (ISO/IEC Guide 73:2009, p. 3-4).

Risk management standards, regulations and recommendations include quite precise definitions to risk management terminology, but rather vaguely use terms related to communication, reporting and the report. It seems that the terminology related to the concept of sharing risk information is not yet very established. Communication is the process by which people exchange information. It is generally an informal, two-way process to convey and receive information, a dialogue of sorts. The risk report is a tool that is used as a means in risk reporting. The report is a written or spoken description of a situation or an event giving people the information they need. Reporting could be seen more as the activity of telling (writing or speaking) people information. In this context, reporting refers to a more formal process of officially disclosing information regarding a specific issue or theme.

AIRMIC, ALARM and IRM's shared way of thinking provides one approach to the semantic issue. Risk reporting provides information on historical losses and trends. However, risk disclosure is a more forward-looking activity that anticipates emerging risks. (AIRMIC et al. 2010, p. 16)

Regardless of the above organizations' definitions, this study does not use the term "disclosure" as a synonym for "report," In this study, it seems irrelevant to separate risk report content into two just because reporting is considered to be related to the past and disclosure to the future. The idea is to look at the risk report concept from a wider perspective.

2.2 List of used abbreviations

AIRMIC = The Association of Insurance and Risk Managers

ALARM = The National Forum for Risk Management in the Public Sector

COSO = Committee of Sponsoring Organizations of the Treadway Commission

EU = European Union

ERM = Enterprise Risk Management

FERMA = Federation of European Risk Management Associations

FIN-FSA = The Financial Supervisory Authority

IFRS = International Financial Reporting Standards

IRM = The Institute of Risk Management

IAS = International Accounting Standards

ISO 3100 standard = Risk Management standard

ISO/IEC Guide 73 = Risk Management - Vocabulary - Guidelines for use in standards

OECD = The Organization for Economic Co-operation and Development

3 Reporting in risk management standards and frameworks

This chapter takes a closer look at the risk reporting concept discussed in the Risk Management Standard, the ERM framework and the ISO 31000 standard.

The Risk Management Standard, first published in 2002, is the result of work by a team drawn from the major risk management organizations in the UK: The Institute of Risk Management (IRM), The Association of Insurance and Risk Managers (AIRMIC) and ALARM (The National Forum for Risk Management in the Public Sector). In 2003, The Federation of European Risk Management Associations (FERMA) published the standard in several European languages. The standard has, wherever possible, used the terminology for risk set out by the International Organization for Standardization's ISO/IEC Guide 73 Risk Management - Vocabulary - Guidelines for use in standards.

The Committee of Sponsoring Organizations of the Treadway Commission's (COSO) published the Enterprise Risk Management (ERM) concept in 2004. The concept provides a framework for undertaking ERM. The term enterprise risk management is used as a description of the comprehensive and holistic approach to risk management and the managing of risk.

The ISO 31000 standard was published in 2009 as an internationally agreed standard for the implementation of risk management principles. The ISO 31000 standard is the first risk management standard in the world.

3.1 Risk Management Standard and risk reporting

According to the Risk Management Standard, good corporate governance requires that companies adopt a methodical approach to risk management

which: protects the interests of their stakeholders, ensures that the board of directors discharges its duties to direct strategy, build value and monitor performance of the organization, ensures that management controls are in place and are performing adequately. The arrangements for the formal reporting of risk management should be clearly stated and be available to the stakeholders. (AIRMIC et al. 2002, p. 10)

The Risk Management Standard emphasizes that a company needs to report to its stakeholders on a regular basis, setting out its risk management policies and the effectiveness in achieving its objectives. Increasingly, stakeholders look to organizations to provide evidence of effective management of the organization's non-financial performance in such areas as community affairs, human rights, employment practices, health and safety and the environment. (AIRMIC et al. 2002, p. 9)

Figure 2 The risk management process, according to the Risk Management Standard (AIRMIC et al. 2002, p. 4)

In addition, the formal reporting should address the control methods – particularly management responsibilities for risk management, the processes used to identify risks and how they are addressed by the risk management systems, the primary control systems in place to manage significant risks, and the monitoring and review system in place. Any significant deficiencies uncovered by the system, or in the system itself, should be reported along with the steps taken to deal with them. (AIRMIC et al. 2002, p. 10)

The Risk Management Standard's approach to risk reporting is based on stakeholder needs. Stakeholders are divided into two groups: internal stakeholders and external stakeholders. Internally, different levels within an organization need different information from the risk management process.

The board of directors

The board of directors should be aware of the most significant risks facing the organization, the possible effects on shareholder value of deviations to expected performance ranges, ensure appropriate levels of awareness throughout the organization, know how the organization will manage a crisis, know the importance of stakeholder confidence in the organization, know how to manage communications with the investment community where applicable, be assured that the risk management process is working effectively, and publish a clear risk management policy covering risk management philosophy and responsibilities. (AIRMIC et al. 2002, p. 9)

Business units

Business units should be aware of risks that fall into their area of responsibility, the possible impacts these may have on other areas and the consequences other areas may have on them, have performance indicators that allow them to monitor the key business and financial activities, progress towards objectives and identify developments that require intervention (e.g. forecasts and budgets), have systems that communicate variances in budgets and forecasts at appropriate frequency to allow action to be taken, report systematically and promptly to senior management any perceived new risks or failures of existing control measures. (AIRMIC et al. 2002, p. 9)

Individuals

Individuals should understand their accountability for individual risks, understand how they can enable continuous improvement of risk management response, understand that risk management and risk awareness are a key part of the organization's culture, report systematically and promptly to senior management any perceived new risks or failures of existing control measures. (AIRMIC et al. 2002, p. 9)

3.2 Enterprise risk management framework and risk reporting

According to the Committee of Sponsoring Organizations of the Treadway Commission (COSO 2004, p. 2), enterprise risk management (ERM) is a process effected by an entity's board of directors, management, and other personnel, applied in a strategy setting and across the enterprise, and designed to identify potential events that may affect the entity. ERM manages risk to be within the risk appetite and provides reasonable assurance regarding the achievement of the entity's objectives.

In the ERM context, risk management is included in management's daily decision making regarding operational activities, strategic planning and implementation, investments, specific projects and business continuity plans.

The ERM framework incorporates corporate governance and internal controls as part of an overall ERM structure. Enterprise risk management consists of eight interrelated components. These are derived from the way management runs an enterprise and are integrated with the management process. Enterprise risk management components represent what is needed to achieve the company's objectives. One of these components is information and communication, underlining that relevant information is identified, captured, and communicated in a form and timeframe that enables people to carry out their responsibilities. (COSO 2004, p. 3-4)

ERM refers to integrated approaches within a common framework to measure and manage risks across the company, as opposed to the past when companies managed risks using a "silo" approach in which different types of risk—strategic, business, credit, market, operational— were managed by different organizational units. By their nature, risks are highly interdependent. (Lam, 2008, p. 4)

Lam (2008, p. 10) highlights that, given the wide scope of ERM, many companies are overwhelmed with their risk identification, assessment, documentation, and reporting processes. The objective of ERM should not be to address all of the risks faced by the company. In fact, it would be impossible to identify all of the company's risks because that list is infinite. The objective of ERM should be to support decisions on the critical risks and opportunities for the board of directors, executive management, and business and operational units. An effective ERM program should prioritize risk information for the company's key decision makers.

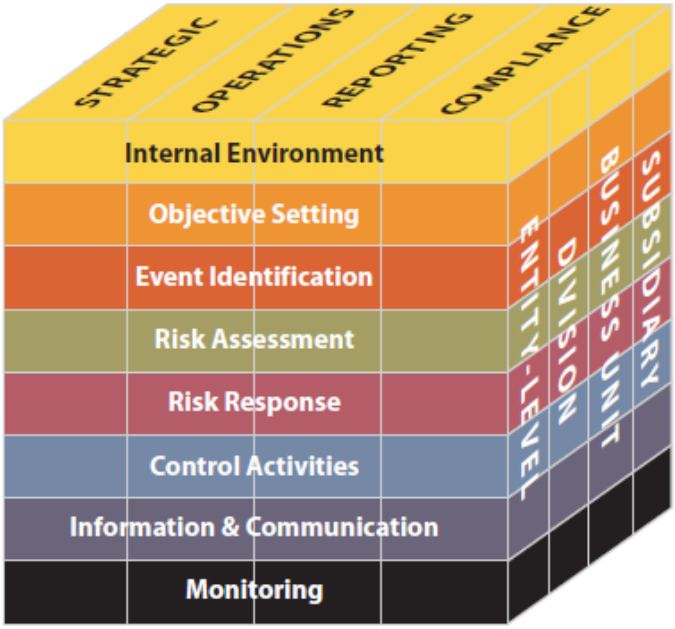

Figure 3 Enterprise risk management framework (COSO 2004, p. 5)

According to the COSO approach, when a company starts to develop risk reporting it should include its communication processes, target audiences, and reporting formats. Organizations should start by keeping things simple, clear and concise. Regardless of what specific reporting format is used, the reporting must reflect clearly the relative importance or significance of each risk. Many organizations use simple lists, with their top risks listed in rank order. Status reporting and tracking needed to monitor the progression of action plans should also be considered so that gaps in risk processes or risk responses identified during ERM implementation can be addressed. (COSO 2011, p. 6)

As far as recommendations and definitions related to risk reporting and communication are concerned, one of the key objectives of ERM is to promote risk transparency, both in terms of internal risk reporting and external public disclosure. Establishing a robust risk measurement and reporting system is therefore critical to ERM success. (Lam 2008, p. 6)

The COSO (2011, p. 10) has also outlined a simple draft of an action plan for implementing ERM, highlighting key events and actions. To start with, a company should assess the adequacy and effectiveness of existing risk reporting. Secondly, a company should develop new reporting formats and consider extensive use of graphics and colors, as well as a risk "dashboard" for the board. Thirdly, a company should develop a process for the periodic reporting of emerging risks. And, finally, a company should assess the effectiveness of new reporting with stakeholders and revise as appropriate.

Hume (2010, p. 369) writes that enterprise risk management is a discipline that allows management to judge total business risks. Enterprise risk management reporting and disclosure provides the forum for discussing the key vulnerabilities and risks of the company and strengthens management accountability. Transparency is important to enterprise risk management disclosure, as management needs to track exposures and discuss these regularly. Without transparency and disclosure, the company lacks the information to make important risk decisions.

3.3 ISO 31000 standard and risk reporting

The ISO 31000 standard Risk Management – Principles and guidelines describes the framework for risk management and the necessary components of the framework.

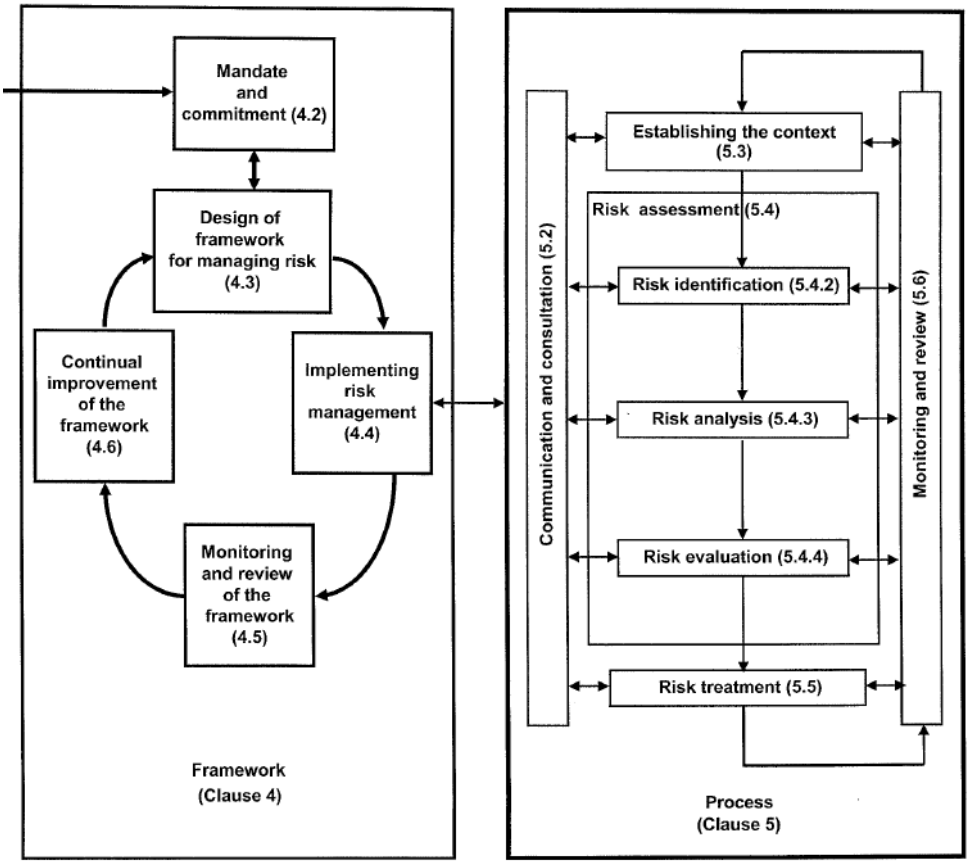

Figure 4 The image depicts the relationship between the risk management framework and processes. In the ISO 31000 standard the communication systems should ensure that key components of the risk management framework are communicated and that there is reporting on the risk management framework, its effectiveness and the outcomes. (ISO 31000:2009, p. vii)

Communication and consultation is presented in the ISO 3100 as part of the risk management process. According to the ISO 31000 standard (2009, p. 12), the organization should establish internal communication and reporting mechanisms in order to support and encourage accountability and ownership of risk.

According to the standard, the internal communication and reporting mechanisms should ensure that key components of the risk management framework are communicated. In addition the mechanisms should ensure that there is adequate internal reporting on the risk management framework, its effectiveness and the outcomes. Furthermore, the mechanisms should ensure that relevant information derived from the application of risk management is available at appropriate levels and times. Accordingly, the mechanisms

should include processes to consolidate risk information from a variety of sources. (ISO 31000:2009, p. 12)

In the ISO context, communication is defined as a continual and iterative process that an organization conducts to provide, share or obtain information and to engage in dialogue with stakeholders regarding the management of risk. The information can relate to the existence, nature, form, likelihood, significance, evaluation, acceptability and treatment of the management of risk. (ISO/IEC Guide 73:2009, p. 3)

In the above ISO context, reporting is defined as a form of communication intended to inform particular internal or external stakeholders by providing information regarding the current state of risk and its management (ISO/IEC Guide 73:2009, p. 12).

In order to ensure that risk management is effective and continues to support organizational performance, the organization should report on risk, progress with the risk management plan and how well the risk management policy is being followed (ISO/IEC Guide 73:2009, p. 13).

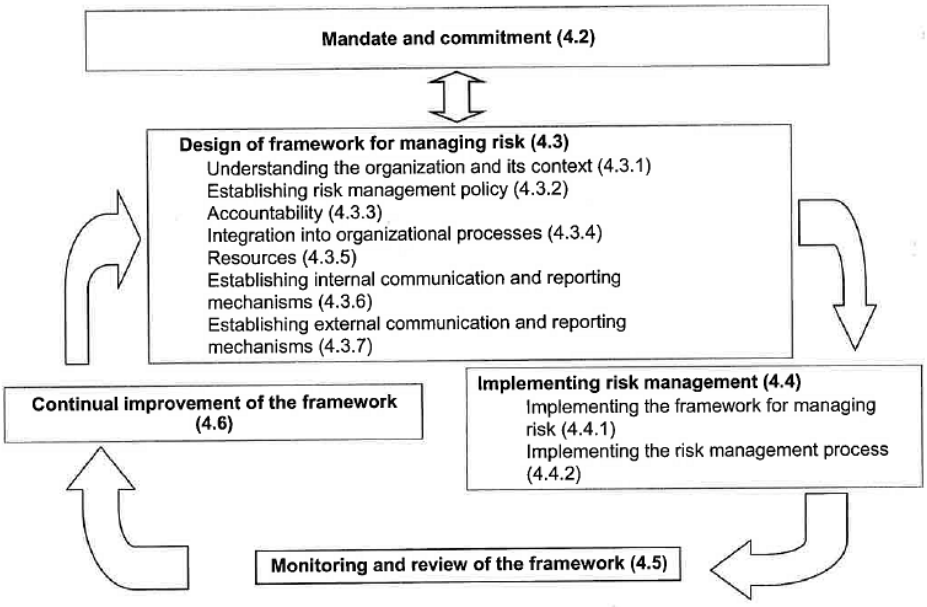

Figure 5 The relationship between the components of the framework for managing risks. Communication and reporting mechanisms are included in the framework design. (ISO 31000:2009, p. 9)

The ISO 31000 standard's (2009, p. 12) view of external communication is that the organization should develop and implement a plan as to how it will communicate with external stakeholders. The plan should involve engaging the relevant 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.

As stated above, the starting point for external communication is that a company complies with laws, regulations and requirements. It is interesting to note that the standard gives a more precise description of the overall content of internal communication and reporting than external communication. From the angle of the study, the finding is quite relevant.

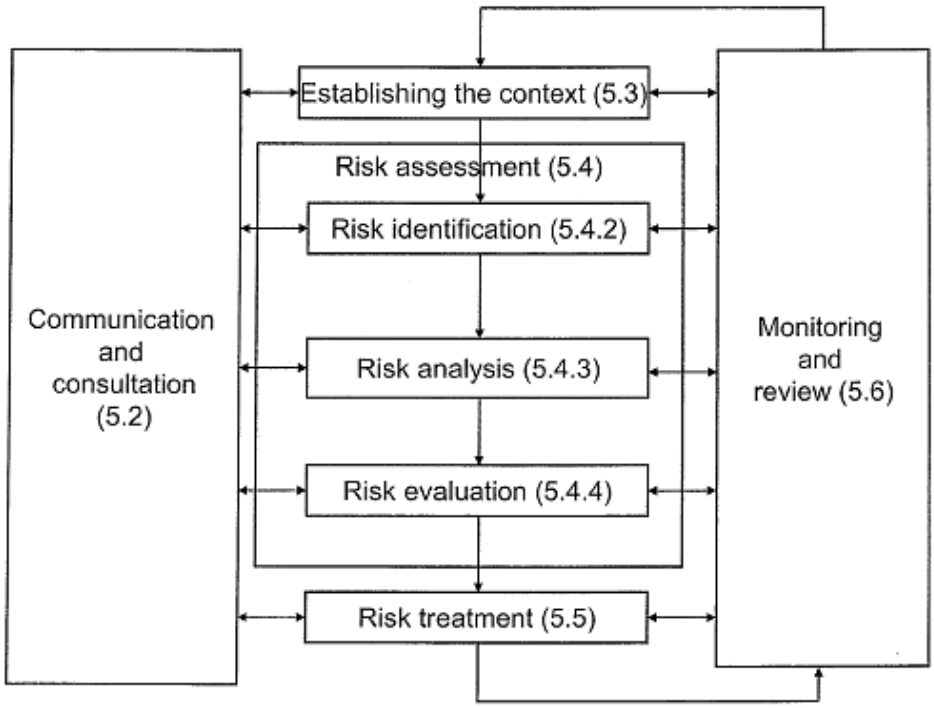

Figure 6 The risk management process showing that communication (and consultation) should be embedded in all stages of the process. (ISO 31000:2009, p. 14)

We've learned that communication is a process to provide, share or obtain information regarding, e.g., the existence, nature, form, likelihood, significance, evaluation, acceptability and treatment of the management of risk (ISO/IEC Guide 73:2009, p. 3). The ISO 31000 standard emphasizes that communication should take place during all stages of the risk management process; the plans for communication should be developed at an early stage and address issues relating to the risk itself, its causes, its consequences (if known) and treatment measures. Effective communication should ensure that those accountable for implementing the risk management process and the stakeholders understand the basis on which decisions are made and the reasons why particular actions are required. (ISO/IEC Guide 73:2009, p. 14)

Communication with stakeholders is important, as they make judgments about risk based on their perceptions of risk. The perceptions can vary due to differences in values, needs, assumptions, concepts and concerns. Above all, communication should facilitate truthful, relevant, accurate and understandable exchanges of information. (ISO/IEC Guide 73:2009, p. 15)

The ISO 31000 standard highlights some characteristics of enhanced risk management. Continual communication is one of them. Based on the standard (ISO/IEC Guide 73:2009, p. 23), enhanced risk management includes continual communications, including comprehensive and frequent reporting of risk management performance as a part of good governance. Communication is seen as a two-way process so that decisions can be made about the level of risks. Comprehensive and frequent reporting both on significant risks and on risk management performance contributes substantially to effective governance within an organization.

4 Reporting in the regulation and control environment

Listed companies need to comply with certain regulations set by the financial markets' supervisory and surveillance authorities. Rules and regulations serve an important purpose: to sustain confidence in the financial market and enable a common framework for listed companies.

In Finland, good corporate governance consists of various factors. There are both statutory regulations and recommendations based on self-regulation. The purpose of corporate governance has been to complement legislation and facilitate the interpretation through the recommendations. The most essential statutory regulation for listed companies is integrated in the Companies Act, the Security Markets Act, the Auditing Act and the Accounting Act. A few EU directives worth noting include the fourth company law directive (annual accounts of companies with limited liability) and the directive on shareholders rights. The European Commission has adopted a recommendation on directors' remuneration and a recommendation on the role of independent directors.

The Corporate Governance Code focuses on transparency and the promotion of governance.

4.1 Regulatory requirements

The rules and regulations issued by the national stock exchange (NASDAQ OMX Helsinki) and the national financial market supervision (Financial Supervisory Authority) include specific information on verbal risk disclosure guidelines. It must be noted that regulatory requirements regarding risk reporting refer solely to external reporting, not internal reporting.

4.1.1 NASDAQ OMX Helsinki regulations

NASDAQ OMX Helsinki – commonly referred to as the Helsinki Exchange – has a variety of rules related to the disclosure of information, of which the most relevant for a listed company are the "Rules of the Stock Exchange and in the NASDAQ OMX Helsinki" and the "Harmonized Disclosure Rules." Apart from rules related to the actual financial statement and general disclosure requirements based on the Finnish Securities Markets Act, there are no specific guidelines or requirements related to risks or risk management. Nor are there guidelines or recommendations for a listed company regarding risk and risk management communication or reporting in the NASDAQ OMX Helsinki.

4.1.2 The Finnish Financial Supervision Authority regulations

The Financial Supervisory Authority (FIN-FSA) is the authority overseeing Finland's financial and insurance sectors. Two standards in its regulations and guidelines related to the disclosure of information by listed company are: "Standard 5.1 Disclosure of periodic information" and "Standard 5.2b Disclosure obligation of the issuer and shareholder."

FIN-FSA describes a standard as a collection of subject-specific regulations and guidelines that obliges and guides supervised entities and other financial market participants, indicates the quality level expected by the supervisor, sets out the supervisor's key principles of good practice and provides justification for regulation (FIN-FSA 5.1:2009, p. 2).

Standard 5.1 Disclosure of periodic information

According to the FIN-FSA Standard 5.1 (2009, p. 30-31), a management report, presenting information on significant matters relating to the development of the reporting entity's operations, must be attached to the financial statements. The standard suggests that the management report includes a description of significant risks and uncertainties. The management report generally describes the extent to which previous assumptions have proved to be correct and previous specified risks have materialized.

The management report must include a balanced and complete assessment with regard to the extent and structure of the operations, of significant risks

and uncertainties, and of other conditions affecting financial performance (FIN-FSA Standard 5.1:2009, p. 34).

The management report should describe the issuer, its operating activities and typical sector risks, uncertainties and other issues that, if realized, may significantly affect the issuer's operations, financial position and performance or the value of the security. If possible, it should also describe the effect that the realization of the risks and uncertainties would have on the issuer. (FIN-FSA Standard 5.1:2009, p. 34)

FIN-FSA Standard 5.1 (2009, p. 34) points out that the description of risks and uncertainties is generally based on an assessment (made at the date of the statement of financial position) of the risks and uncertainties attributable to the next financial period. If, however, the issuer knows of such risks and uncertainties that may be realized over a longer term than the immediately subsequent financial period, these risks and uncertainties, too, are generally included in the description.

According to FIN-FSA Standard 5.1 (2009, p. 34), the effects of the risks and uncertainties may be described by means of various kinds of sensitivity analyses, which, depending on the issuer's line of business, can be used to illustrate how key factors, such as exchange rates or other individual factors, affect financial performance and/or position.

Risks affecting the issuer can be broken down into strategic risks, operational risks, financial risks and damage risks, for example. Depending on the issuer's line of business, environmental risks may also be significant and topical. In addition, the issuer may be exposed to credit, liquidity and market risks attributable to financial instruments. Certain sectors may have standardized risk ratings that can be used in describing the risks. (FIN-FSA Standard 5.1:2009, p. 34)

In addition, the guideline related to disclosure of order backlog and related risks states that the management report must include the order backlog and the related essential risks at the end of the financial period to the extent that they have not been taken into account in the financial statements. Information deemed essential must be disclosed. The order backlog disclosed generally includes those binding, outstanding orders that have been received by the date of the statement of financial position but not yet recognized as

revenue, according to IAS 11 Construction Contracts. (FIN-FSA Standard 5.1:2009, p. 36)

According to FIN-FSA Standard 5.1 (2009, p. 58-59), a company should publish an explanatory statement in its interim reports. The explanatory statement should give a general description of the financial position and result of the issuer and of developments during the report period. The explanatory statement should explain any material events and transactions of the report period and their impact on the financial position and result of the issuer. The description of principal short-term risks and uncertainties relating to the business operations should focus particularly on material changes that have occurred in the risks and uncertainties previously disclosed in connection with the financial statements. As regards the detailed description of risks and uncertainties, the explanatory statement can include references to disclosures in the management report.

Standard 5.2b Disclosure obligation of the issuer and shareholder

According to FIN-FSA Standard 5.2b (2010, p. 20), when a company is presenting its assessment on likely future performance, it should pay attention to significant near-term risks and uncertainties of its business operations and rely on estimates with solid rationale.

4.2 Governance and control requirements

4.2.1 The Finnish Corporate Governance

One of the most fundamental guidelines related to risk management as well as risk reporting among Finnish listed companies is the Finnish Corporate Governance Code. In 2003, the Securities Market Association issued the Corporate Governance Recommendation for Listed Companies. The Recommendation was replaced by the Finnish Corporate Governance Code in 2008. The Code was updated in 2010. The target of the Recommendation and later the Code is to improve the corporate governance practices of Finnish companies and to improve external stakeholders' access to information about the corporate governance system as a whole.

The Finnish Corporate Governance Code (2010, p. 6) has been prepared in accordance with the so-called Comply or Explain principle. This means that the company shall comply with all recommendations of the Code. A com-

pany may depart from an individual recommendation, but if it does, it must account for the departure and provide an explanation for it.

It should be noted, however, that risk management's role and tasks in the Code are defined in relation to the financial reporting process.

In compliance with the Code, the board of directors should establish board committees for the effective discharge of duties of the board. One of the recommended committees, the audit committee, has a special role in risk management. Among other things, the audit committee shall monitor the efficiency of the company's risk management systems and review the description of the main features of the risk management systems pertaining to the financial reporting process, which is included in the company's corporate governance statement. (Securities Market Association 2010, p. 15)

According to the Code (2010, p. 22), the purpose of internal control and risk management is to ensure the effective and profitable operations of the company, reliable information and compliance with the relevant regulations and operating principles. Another aim is to be able to identify, evaluate and monitor risks related to the business operations.

According to Recommendation 49, the company shall disclose the major risks and uncertainties that the board is aware of and the principles along which risk management is organized (Securities Market Association 2010, p. 22).

For the evaluation of the operations of the company, it is important to provide sufficient information on risk management. Legislation requires that the report by the board of directors contain an evaluation of the major risks and uncertainties. In addition, the interim reports and financial statements releases shall describe major short-term risks and uncertainties related to the business operations. (Securities Market Association 2010, p. 22)

According to Recommendation 54, listed companies must issue a Corporate Governance Statement describing the main features of the internal control and risk management systems in relation to the financial reporting process. The description outlines the manner in which the company's internal control and risk management function is organized in order to ensure that the financial reports disclosed by the company give essentially correct information

about the company finances. The description is given at the group level. (Securities Market Association 2010, p. 25)

As far as general investor information is concerned (Recommendation 55), the company should present on its website the principles along which risk management is organized and the major risks and uncertainties that the board is aware of. (Securities Market Association 2010, p. 26)

4.2.2 European Commission Corporate Governance Framework

The European Commission has issued a Green Paper on "The EU Corporate Governance Framework" aiming to promote good corporate governance across Europe.

A green paper released by the European Commission is a discussion document intended to stimulate debate and launch a process of consultation, at the European level, on a particular topic. A green paper usually presents a range of ideas and is meant to invite interested individuals or organizations to contribute views and information.

Risk management issues in the European Commission's green paper "The EU Corporate Governance Framework" are covered only in connection with the board's oversight responsibilities and administrative tasks. The framework advises all companies to develop an adequate risk culture and arrangements to manage risk effectively and stresses that the board should ensure a proper oversight of the risk management processes (EU Corporate Governance Framework 2011, p. 10). However, the paper does not mention any risk reporting activities or principles whatsoever.

4.2.3 OECD Principles of Corporate Governance

The Organization for Economic Co-operation and Development (OECD) published "OECD Principles of Corporate Governance" as early as 1999 and a renewed version in 2004. The principles document offers non-binding standards and good practices as well as guidance on implementation of good corporate governance practices.

The OECD principles (2004, p. 11) are intended to provide guidance and suggestions for stock exchanges, investors, corporations, and other parties

that have a role in the process of developing good corporate governance. The principles focus on publicly traded companies.

The document describes risk-related information under the headline “Foreseeable risk factors,” stating that users of financial information and market participants need information on reasonably foreseeable material risks that may include: risks that are specific to the industry or the geographical areas in which the company operates; dependence on commodities; financial market risks, including interest rate or currency risk; risk related to derivatives and off-balance sheet transactions; and risks related to environmental liabilities. (OECD 2004, p. 54)

The document emphasizes that the principles do not envision the disclosure of information in greater detail than it is necessary to fully inform investors of the material and foreseeable risks of the enterprise. Disclosure of risk is most effective when it is tailored to the particular industry in question. Disclosure about the system for monitoring and managing risk is increasingly regarded as good practice. (OECD 2004, p. 54)

4.3 Statutory requirements

Laws, such as the Finnish Companies Act, the Finnish Accounting Act, and the Finnish Securities Markets Act, are reviewed for the study, bearing in mind, however, that the content of such statutory requirements focuses on financial accounting and reporting practices. Nevertheless, it is worth looking at what, if any, verbal risk reporting content is covered in the above-mentioned laws.

The Finnish Companies Act (21.7.2006/624) does not include any mention related to risk, risk management or risk reporting.

According to the Finnish Accounting Act 3:1§ (30.12.1997/1336), a company must comprehensively evaluate its key risks and uncertainties.

The Finnish Securities Markets Act (14.12.2012 746/2012) states that a company must disclose a description of the key near-future risks and uncertainties related to its business operations.

5 General reporting recommendations

In addition to the previously covered material, a short review of existing studies and publications related to the risk reporting concept is worthwhile. Several risk management associations and global business and management advisors have published their considerations regarding risk reporting.

5.1 Risk reporting definitions of risk management associations

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) highlights the ERM approach in risk report stating that: Risk management processes that capture risk information from each level of the organization aid in the creation of a composite view of key risk exposures for presentation by management and discussion with the board. A portfolio view of risks informs management and the board about concentrations of risks affecting specific strategies or overlapping risk exposures for the enterprise and helps in the prioritization of the enterprise's top risk exposures based on assessments of risk probabilities and impact to the organization. (COSO 2009, p 14)

According to the COSO's view (2009, p. 16) the organization's ERM system should function to bring to the board's attention to the most significant risks affecting entity objectives and allow the board to understand and evaluate how these risks may be correlated, the manner in which they may affect the enterprise, and management's mitigation or response strategies.

The COSO (2009, p. 17) gives an example of the types of information that may be warranted for board review:

• External and internal risk environment conditions faced by the organization

• Key material risk exposures that have been identified

• Methodology employed to assess and prioritize risks

• Treatment strategies and assignment of accountabilities for key risks

• Status of implementation efforts for risk management procedures and infrastructure

• Strengths and weaknesses of the overall ERM process

Heat maps are one type of tool that can provide an effective visualization to help direct the board and senior management discussion to those risk issues that are critical to the organization. Other tools exist that can help management and the board understand the portfolio of key risk exposures. The use of such tools should be tempered by the realization that many of the risk events that played a significant role in prior financial crises are best characterized as low likelihood/frequency, but extremely high impact occurrences. These so-called “tail events” or “black swans” have proved to be extremely worthy of board attention and oversight. (COSO 2009, p. 14)

The Institute of Operational Risk (2010, p. 15) stresses the importance of a coordinated risk report. The scope, content and presentation of a report will depend on the requirements of the intended audience and where possible reports should be developed in conjunction with them. However, central coordination can help to ensure that a consistent view of information is delivered so that the reports can be compared across business lines and functions and/or aggregated for senior management.

The following diagram of the Institute of Operational Risk illustrates the main levels of operational risk reporting that most organizations may wish to consider:

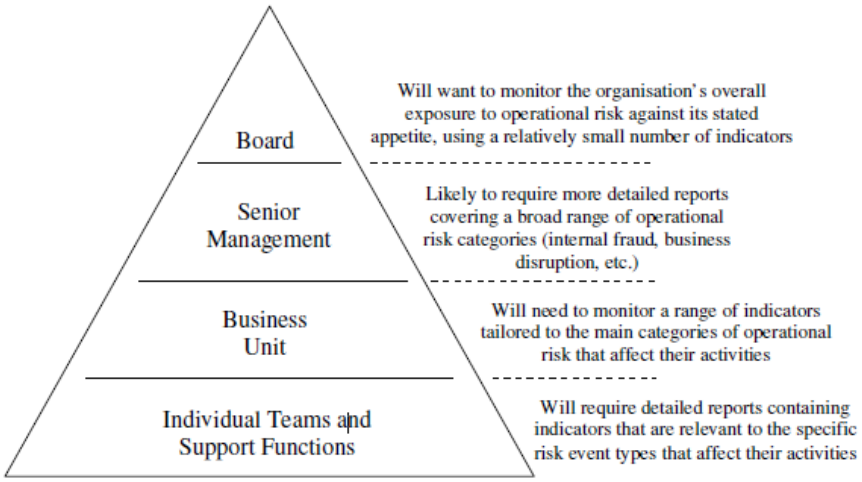

Figure 7 The four main levels of operational risk reporting (Institute of Operational Risk 2010, p. 15)

5.2 Risk reporting definitions of business consultant companies

In its global survey, the insurance brokerage AON (2010, p. 3) has listed key internal and external stakeholders' questions related to risk management: "What are your top risks? How are you going to manage these risks? How is the organization's risk profile changing? Which business lines bring the most risk? What is the potential financial impact of key risks? What is your risk appetite and tolerance? Have you allocated your resources the way to manage key risks? Do employees understand their risk management roles? How is risk incorporated into strategy development? The list demonstrates the wide scope of the risk information that company stakeholders are interested in.

AON (2010, p. 5) also recommends companies to provide board members with ongoing information about risk management best practices and encourage an understanding of risk assessment as a visible aspect of business planning, operations and risk monitoring. Furthermore, AON (2010, p. 7) encourages company top management to consider, at least once a year, both new and emerging risks in the context of the organization's strategic plan, operating plan, and external environment.

AON defines transparency of risk communication as one of the hallmarks of a successful ERM approach. Internal and external stakeholders are requiring increased information about risk to support their own decisions regarding how to manage their risk while also understanding how risk across the value chain can affect business objectives and ultimately performance (AON 2010, p. 6).

AON's (2010, p. 6) advice concerning risk communication is to "customize risk reporting and communications to gather and deliver the right information to the right people at various levels of the business." The other advice encourages streamlining data reporting by focusing on the most critical risks and decision points. Companies should use a risk dashboard approach that delivers relevant information at various levels of the organization to support risk-based decision making. According to the AON survey, managing risk disclosures requires an understanding of what each group of stakeholders expects and how the information will be used.

According to PwC (2012, p. 42), the purpose of a risk report is to facilitate risk monitoring by providing necessary information and analysis of the existing and potential risks to which the company is exposed. The content of the risk report must be adapted to its readership. For senior management: a risk report presents, in about ten pages, an overview of the risks affecting the company (the risk map, the three to five major risks, the market environment, and comparisons with competitors). For the business line or operational entity: the risk report covers, in about 15 pages, the risks to which the business line or operational entity is exposed. The detailed risk report, often about 100 pages or more, provides all the evaluations and detailed action plans for each risk.

6 Key findings of the risk reporting concept

6.1 RM standards and ERM framework reporting

Segal (2011, p. 271) calls risk reporting “risk messaging” and divides it into internal and external risk messaging. According to Segal, internal risk messaging refers to incorporating risk information into performance measurement and management. Internal risk messaging has two aspects: 1) integrating ERM into business performance analysis, and 2) integrating ERM into incentive compensation.

Another theme addressed by Segal is the reporting of the integrated impacts of two or more risk scenarios occurring simultaneously. Though Segal uses the following example in connection with external risk reporting, it is worthy of consideration also in internal risk reporting: the strategic focus of the ERM program and how it focuses management on the largest potential threats, whether from a single risk event or from combinations of simultaneous risk events (Segal, 2011, p. 281).

When designing the format and content of an ERM report, and the functionality of an ERM reporting system, it is important to start by looking at the five basic questions that an ERM reporting system should address: 1) Are any of our business objectives at risk? 2) Are we in compliance with policies and regulations? 3) What risk incidents have been escalated? 4) What KRIs and trends require immediate attention? 5) What risk assessments need to be reviewed? With an effective ERM reporting system, management should be able to answer all five of these questions. (Lam 2008, p. 6)

According to Lam (2008, p. 10) many ERM programs produce large volumes of qualitative information (e.g., risk and control assessments, process maps, policies and procedures) that are not conducive to board and man-

agement decision making. In order to support policy and business decisions, critical risks must be quantified and reported in a concise and effective manner. That is not to say that quantitative information is more valuable than qualitative data, but there should be a balance in ERM reporting. For the company's most critical risks, quantitative analysis can be used to show trends, risk-adjusted metrics, compliance with policy limits, and performance against established standards. For the same risks, qualitative analysis can be used to provide expert risk assessments, alternative strategies and actions, management recommendations, and other contextual information.

6.2 General reporting recommendations

It is quite obvious that risk reports provide essential information for the decision makers across the company. From management's and control's viewpoint, it is vital that top management's risk reports follow a systematic schedule and structure. For example, key opportunities and threats are reported quarterly, and changes in the risk levels and risk management activities are reported monthly. In practice, the focus of top management risk reporting is shifted to the monitoring of risk management activities and their impact, and the estimation of the future based on risk development trends. (Ilmonen et al. 2010, p. 188)

PwC (2012, p. 42) has stated that if the company is using risk measurement tools and processes, the risk management system must produce all the information necessary to the relevant managers to ensure appropriate and hands-on oversight.

Ilmonen et al. (2010, p. 188-189) writes that the internal risk management reporting may include an operational risk management report reporting near-miss incidents and hazards. In practice, the ERM report is updated 1-4 times per year and its focus is on strategic and partially financial risks. Financial risk reporting has its own long tradition and financial risks will be reported separately in the future, too.

There is not one right risk reporting model, and companies have to plan the risk reporting in detail – keeping in mind that it must create as much value added as possible (Ilmonen et al. 2010, p. 193).

As a result of numerous legislative and regulatory requirements, the expectations for more effective risk oversight by the board are being raised. Accordingly, based on Protiviti's survey "Board risk oversight" (2010, p. III), risk oversight is a high priority on the agenda of most boards. The respondents included more than 200 current and past board members from a broad range of industries and organizations in the USA.

Based on the survey (Protiviti 2010, p. 7), the most common types of risk reporting received by the board annually include: 1) a high-level summary of top risks for the enterprise as a whole and its operating units; 2) a periodic overview of management's methodologies used to assess, prioritize and measure risk; and 3) a summary of emerging risks that warrant board attention. The risk reporting not received annually include: 4) a scenario analyses evaluating the impact of changes in key external variables impacting the organization; 5) a summary of exceptions to management's established policies or limits for key risks; and 6) a summary of significant gaps in capabilities for managing key risks and the status of initiatives to address those gaps. The findings reveal an opportunity for organizations to improve the risk reporting process and increase the regularity of reporting according to the nature of the organization's operations and risk profile as well as the board's specific needs. The other three report types mentioned by the respondents are: 7) risk reports, such as trends in key risk indicators; 8) a report on effectiveness of responses for mitigating the most significant risks; and 9) a summary of significant changes in the assumptions and inherent risks underlying the strategy and their effect on the business.

The role of the board in the risk management process usually means that the board determines that management has in place a rigorous process for identifying, prioritizing, managing and monitoring its critical risks and that this process is improved continuously as the business environment changes. It also involves the board's understanding of the most significant risk exposures and evaluation of whether those exposures are within the company's appetite for risk-taking. (Protiviti 2010, p. 4)

According to the survey respondents, there should be a structured process for monitoring and reporting key risks to the board, and that the board has overall responsibility for risk oversight. They call for a more robust and mature process, referring to a process that is repeatable over time, well-

defined, supported by rigorous methodology and analytical frameworks and applied periodically over time as opposed to on an as-needed basis. (Protiviti 2010, p. 4-5)

Recommendations listed in the Protiviti survey (2010, p. 15) state that there are opportunities to improve the maturity of the board risk oversight process so that it can become more systematic, robust and repeatable. A company may implement a more structured process for reporting critical enterprise risks and emerging risks to the board, and look for opportunities to enhance the risk reporting process to make it more effective and efficient, as well as increase the regularity of reporting depending on the nature of the organization's operations and risk profile. And it may come to an agreement with management on the risk-related matters that need to be escalated to the board, addressing the what, when and why.

The Institute of Operational Risk states that the prioritization of risk indicators helps information consumers to focus on those indicators (and their associated operational risks) that are most significant for their organization. The Operational Risk Manager's judgment on what to include or exclude from a report may also be necessary to help information consumers reach the right conclusions. However, information consumers and auditors should be able to access data on all available indicators, on request, so that they can satisfy themselves that the most appropriate indicators have been presented. The provision of a suitably detailed narrative to support the figures is critical to ensure that information consumers are able to interpret the reports that they receive and use them to support decision making. In particular, brief and relevant commentary should be provided to explain abnormal items and data trends. (Institute of Operational Risk 2010, p. 16)

Institute of Operational Risk (2010, p. 15-16) has listed some features of a sound indicator report/reporting process, including:

• Relevance – care must be taken to avoid producing overly detailed reports with large numbers of indicators;

• Simplicity – reports should not be overly complex and contain jargon terms, large tables of data or complex mathematical formulae. Where possible the simplest possible graphs and charts should be used;

• Timeliness – reports should be produced in a timely manner so that they can be acted upon whilst the data they contain is still relevant;

• Accuracy – inaccurate metrics will provide a false picture of an organization's exposure to operational risk and may mean that it ends up over-exposed or invests too much in reducing certain risks. Processes should be in place to check the accuracy of reported metrics on an ongoing basis;

• Trending – reports should make clear the historical trends of the chosen indicators to provide some indication of their volatility and/or where they may be heading;

• Clear escalation procedures – so that the recipients of a report know when to escalate areas of concern to more senior management; and

• Compliance – with any regulations that may exist, where appropriate.

Questions related to the reporting frequency and presentation style are far less important than the content, but they form a basis for the whole report concept. According to the Institute of Operational Risk, there is no right answer to the frequency of reporting. It will depend on the nature of the risks, indicators and environment. Reporting should be linked to the timeliness of decision making, and action formulation and reports of different frequency will be required to suit specific audiences. (Institute of Operational Risk 2010, p. 16)

The top management's risk report must follow a regular timetable and structure. Kuusela & Ollikainen (2005, p. 188) suggest separating reports into two based on their content. One option is to divide the management risk report so that the most important threats and opportunities are reported quarterly, and the changes in risk levels and risk management activities are reported monthly.

A company's most significant risks do not change frequently, but their impact and probability may alter and cause changes in the risk management activities. In practice, the focus of the top management risk reporting has shifted to monitoring the risk management activities and their impact and to anticipating the development trend of the risks. (Kuusela & Ollikainen 2005, p. 188)

Lam (2008, p. 11) emphasizes that an ERM report should not be a 50-page report that takes the board two hours to simply walk through. A common complaint from board members and senior executives is that they cannot see "the forest from the trees." Bearing in mind that both the board and the executive management constantly have a number of issues on their daily agenda, a short and simple report is probably the most appreciated.

7 Internal ERM report concept

The name of this study “Concept for an internal enterprise risk management report” implies that the content will cover a range of risks and risk management activities under the same umbrella, giving a comprehensive overview to a company’s most relevant threats and opportunities. Internal refers to the fact that the report contains internal (or even confidential) information that will never be disclosed externally. Internal includes implications that internal target groups are carefully defined and limited to a certain level of the company’s executives, which are responsible for strategic planning and strategy implementation. Besides the content and target groups, the concept reasoning contains structural and frequency aspects.

The starting point is that a company’s corporate-level risk management function both accumulates and retains a great deal of risk information, making it challenging to decide what risk information is needed at different levels of the organization. A commonly used approach is to evaluate the information needs from the target groups’ viewpoint. What are the main responsibilities of a certain target group and what does it try to accomplish? What is their so-called job description? What are they accountable for? With good insight into the target group’s responsibilities and obligations, the definition of content becomes easier. Instead of a generic, one-fit-for-all report concept, different target groups – even within a single company – need different levels of information. The board is generally satisfied with an overall summary delivering a general view on the company’s risk profile, development trends of the most critical risks, and the owners of the risk and risk management operations. The executive management requires more tangible details about the risk, including monitoring of the most significant strategic and operational risks facing the company.

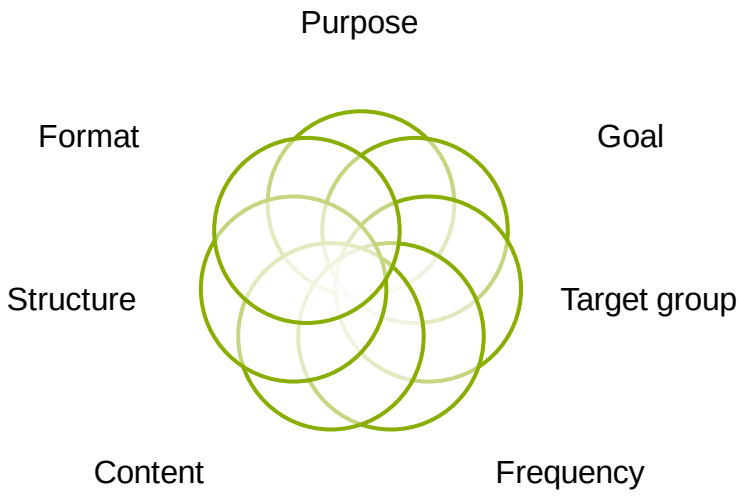

Figure 8 The elements of an internal risk report framework

7.1 Purpose and goals of the risk report

The target of risk reporting is to increase the awareness and transparency of risks and improve the operational efficiency and value creation, as well as to confirm to the target groups that the company's key threats and opportunities are understood and effectively managed and exploited.

The ultimate goal of the risk report – as is the goal of all internal board and executive-level information – is to support the top management in their decisions regarding the managing of the company risks while also understanding how risks across the value chain can affect business objectives and, ultimately, performance.

The risk report must provide such relevant information that it allows the top management to judge total business risks regarding the strategy implementation. Furthermore, it must provide a forum for discussing the key vulnerabilities and risks of the company.

All in all, the internal risk report should try to answer the following questions:

1. What are the company's top risks?

2. How is the company going to manage these risks?

3. How is the company's risk profile changing?

4. Which businesses bring the most risk?

5. What is the potential financial impact of key risks?

6. What is the company's risk appetite and tolerance?

7. Has the company allocated resources to manage key risks?

8. How is risk incorporated into strategy development?

9. Are any of the company's business objectives at risk?

10. What risk incidents have been escalated?

7.2 Internal reporting criteria

Internal reporting criteria describes the key principles that guide risk reporting and helps to create concise content, bring systematization to regular reporting and increase the transparency. They also improve predictability of the reporting in the eyes of the board and executive management, as they are aware of the selection fundamentals.

There are seven identified internal criteria for the risk report:

1. Credibility (based on facts and the knowledge of the best internal and external experts available)

2. Relevance (relates to strategic and business objectives and enables the board and executive management to "see the forest from the trees")

3. Simplicity (avoids complexity, jargon terms, extensive tables of data and mathematical formulas)

4. Timeliness (is produced in a timely manner and is linked to the timeliness of the target groups' decision making whilst the information is still appropriate)

5. Accuracy (uses verified and regularly checked metrics to provide a truthful portrayal of a company's exposure to risks)

6. Regularity (systematic reporting according to the nature of the organization's operations and risk profile as well as the board's specific needs)

7. Trending (clearly shows the historical trends of the chosen risks to give certain indication of their volatility and development path)

Figure 9 Risk report's internal criteria facilitate concise content

7.3 Target groups and report frequency

The key is to customize the risk reporting framework to compile and deliver the right information to the right people at various levels of the business in a company. It is just as important to adjust the risk report concept to the individual target groups' information needs. As stated previously, each target group's responsibilities create a basis for the information scope. The board is satisfied with overall level of risk and risk management information, while the executive management requires more tangible details about the risks facing the company.

Furthermore, it is important to understand the role of each internal target group (the board, the executive management) related to the company's decision making and strategy implementation, as this makes it easier to recognize the level and scope of risk and risk management information needed at different levels of the organization.

Based on the key findings, it is recommended that the corporate-level risk management function prepares two risk reports: one for the board (or the audit or risk committee, depending on the company's governance bodies) and one for the executive management.

Report frequency highly correlates to the company's size, business scope, industry and geographical expansion, and to the risk management itself. Companies that operate in fields prone to vulnerabilities need to report risks and risk management activities more often than companies operating in less complex environments. The annual key processes of risk management, especially risk assessments, contribute to the reporting frequency. If the risk management function makes corporate-level risk assessments once a year, it will report the results once a year. The overall risk management in listed companies is at a good level so the need for the board to read/hear risk overviews could be satisfied with one comprehensive but short risk report annually. The perfect timing for this could be just before the company's annual strategic planning starts. The executive management with its strategy implementation responsibilities requires up-dated risk information more often than the board. Depending on the company's annual management – and risk management cycle – the risk report could be presented bi-annually or quarterly.

7.4 Content of an internal risk report

The overall content of the internal risk report naturally is based on the scope of the company's risk management activities, particularly risk assessments and risk ratings. In the corporate-level risk reporting concept, it is presumed that the report captures risk information from each level of the organization to create a composite view of key risk exposures.

Based on the risk management standard ISO 31000 (2009), a risk is an effect of uncertainty on objectives. In risk assessments, the uncertainty factor of the future is strongly connected to a company's strategy implementation. While assessing future threats and opportunities, a company seeks to evaluate factors that may endanger or enhance the future success of the company: risk is either an opportunity for benefit or a threat to success, or a combination of both aspects.

The two most essential questions in outlining the content for a systematic internal risk report are: 1) What are the uncertainty factors of the future related to the strategy implementation, and 2) How does a company respond to them?

The content of the risk report could be divided into five sections.

Section one discusses the overall performance of the company's risk management activities. This section is seamlessly connected to the board's oversight duty, according to which the board needs to be assured that the company's risk management processes are working effectively. The board monitors the efficiency of the risk management systems and reviews the description of the main features of the risk management systems. It could also be beneficial to briefly recap risk management principles and the methodology used to assess, prioritize and measure risks. Some companies regularly conduct self-evaluations and audits concerning the status of their risk management processes and practices, e.g. business impact analyses, logistics reviews, health, safety & environment audits, and fire & business interruption assessments, the results of which are combined in the corporate-level risk reports to give an overall view of the company's risk management performance.

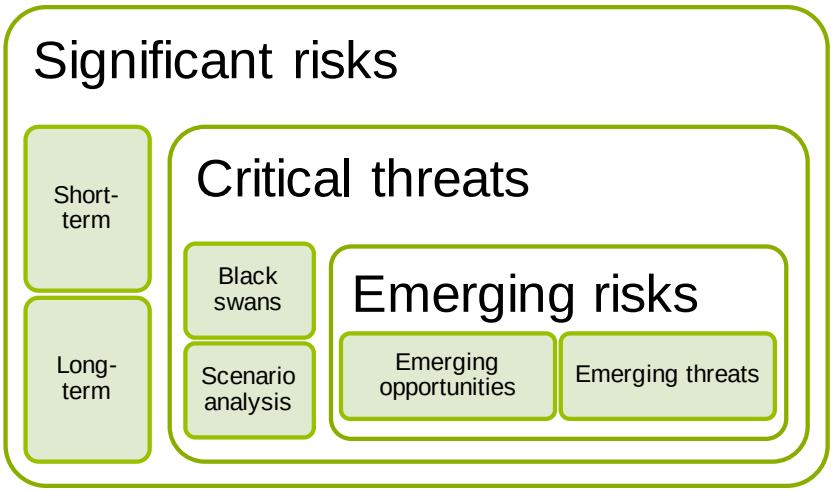

Figure 10 The content of an extended risk description in the risk report

Section two concentrates on risks and it is the widest part of the internal report. The board should be aware of the most significant threats and oppor-

tunities facing the company and affecting the company's objectives. The most significant risks are the ones that can have a direct or indirect material effect, usually adverse, on the company's business, financial situation, operating results or the value of the shares. The material risks are usually related to the company's strategic priorities. To keep the report simple, clear and concise, it is generally enough to include the top 10 (or at most the top 15) risks and their previous ranking position, including a short description of their causes, consequences (if known) and treatment measures. If the company's risk assessment systems allow, the significant risks could be separated under two headlines: short-term risks and risks that may be realized over the long term.

Companies with advanced risk assessment methodologies can show risk trends in the report – for instance, to what extent previous assumptions have proved to be correct and previous specified risks have been realized. The angle should focus particularly on material changes that have occurred in the risks and uncertainties previously disclosed. Whenever applicable, the report should allow the board to understand and evaluate how these risks may be correlated.

Section three covers critical threats (also called "tail events" or "black swans"); these are random events that are highly improbable but would have a huge impact. They are nearly impossible to predict, although the reporting of the integrated impacts of two or more threat scenarios occurring simultaneously could contribute to broader insight of the possible black swans. These critical threats are extremely worthy of board attention and oversight.

Section four highlights the possible new and emerging risks that warrant board attention. The board should be aware of weak signals related to a change in risk development trends. What threats and opportunities have gradually increased their impact and probability, compared to the previous risk assessment?

Section five briefly covers the actions that have been taken to adequately manage the risks and to ensure the continuity of business operations and continuous improvement in the company's overall performance.

Figure 11 The risk report's content elements

The executive management risk report usually contains the same information that is delivered to the board, but it can be deepened with details covering a broad range of strategic and operational risk categories. In addition, the content of the report can be complemented with treatment strategies and the assignment of accountabilities for key risks.

Since corporate-level enterprise risk management activities is a focal point, the inclusion of a short review of the most relevant and significant risk management evaluation results, insurance issues as an integral part of risk treatment measures, and crisis or incidents must be considered. This naturally depends upon the risk management function's responsibilities. If they're included in the scope, insurance issues, crisis situations and corporate security issues easily fall in the executive management's risk report. Especially key findings and preparedness for the similar cases in the future might be more useful for those who are responsible for the strategy implementation.

One consideration that was mentioned in the reference literature relates to competitor information. Comparison with competitors is a point worthy of consideration regarding the content of a risk report. Utilizing business intelligence information and market research, the company could easily find out what risks its competitors face.

7.5 Structure and format of an internal risk report

The structure of the risk report naturally depends on the content. The reference literature used in this study did not cover any structural aspects of the risk report. Therefore, a general report structure can be applied to the risk report structure. A cover page works as the title page. It includes the title, the name of the target group (the board or the executive management) to whom it is being submitted, the date of submission, the name of the person and organization who has prepared the report.

The table of contents gives a clear, well-formatted list of all the sections and sub-sections of the report. The headings of the contents correspond with those in the main body. The table of contents usually reveals what the report is going to be about.

The main body is the actual substance of the report. The structure varies depending on the nature of the material being presented, with headings and sub-headings used to clearly indicate the different sections.

The summary is a brief outline of the report's key findings and main conclusions.

The final part of the report comprises additional material or so-called appendices. This could be detailed documentation or supplementary information that is too long or complicated or not relevant enough to be included in the main body, but should still be of interest to the target groups.

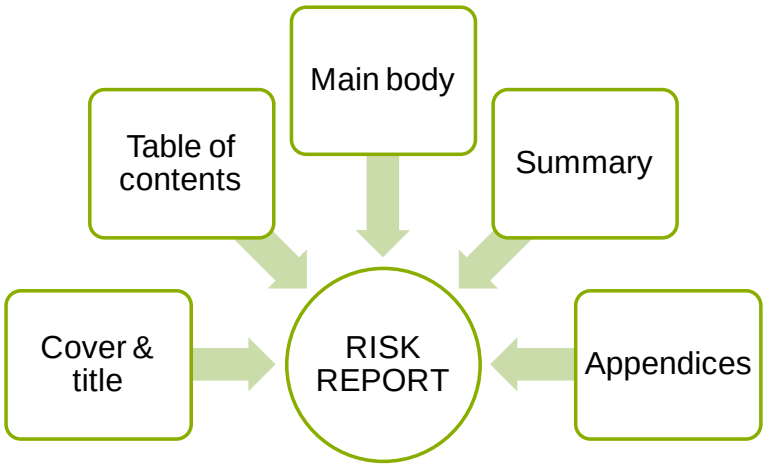

Figure 12 An internal risk report structure

Content is more important than the format, despite the fact that a skillfully made presentation is considered to convey the message more effectively than a hard-to-read 50-page text. A verbal presentation complemented with a concise, written report and clarifying illustrations could be the most practical solution. One possibility is to use heat maps to provide an effective visualization supporting the top management discussion on the risk issues critical to the organization. PowerPoint slides or equivalent presentation formats work well for this purpose, assuming that the content is first explained verbally. If the option is the written report excluding verbal interpretation, a written report is better as it allows longer explanations and a fluent narrative.

8 Conclusions

The term enterprise risk management is used to describe a comprehensive and holistic approach to risk management and the managing of risk. Provided that a company has adapted the enterprise risk management approach regarding all corporate-wide risk activities, the content of the risk report reflects the nature and extension of the ERM.

Risk reporting is an indispensable part of the risk management process. It is a systematic process to inform stakeholders on issues related to risks and risk management, increase the awareness and transparency of risks, and improve operational efficiency and value creation.

There are no specific requirements for internal risk reporting set by statutory or compliance authorities, as internal risk reporting is widely considered to be inherent within the company itself and its businesses. A commonly used approach is to evaluate the information needs from the target groups' viewpoint. With good insight into the target group's responsibilities and obligations, the definition of content becomes easier.

Relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. It's also crucial to ensure that risk reporting is not a one-way flow of information; it should be linked back to those truly accountable for managing risk on various business levels.

The overall content of the internal risk report is naturally based on the scope of the company's risk management activities, particularly risk assessments and risk ratings. In brief, an ideal board-level risk report consists of relevant information about risk management performance, short- and long-term threats and opportunities, critical threats, emerging risks and risk treatment overview.

In addition to this formal top-management risk report, the risk management function should consider the more informal continuous reporting regarding the issues and crisis the company is – often unexpectedly – facing. Many risk management functions already report regularly within the organization on events under their scope within the department's weekly and monthly meetings, for instance.

It's worth noting that even if guidelines and recommendations give a good basis for risk reporting in general, they only indicate the so-called minimum requirements. It is the company itself that further develops both internal and external risk reporting.

9 References

Act 14.12.2012/746. Arvopaperimarkkinalaki (The Finnish Securities Markets Act). The referenced Finnish version accessible at http://www.finlex.fi/fi/laki/ajantasa/2012/20120746?search%5Btype%5D=pika&search%5Bpika%5D=arvopaperimarkkinalaki

Act 21.7.2006/624. Osakeyhtiölaki (The Finnish Companies Act). The referenced Finnish version accessible at http://www.finlex.fi/fi/laki/ajantasa/2006/20060624?search%5Btype%5D=pika&search%5Bpika%5D=osakeyhti%C3%B6laki

Act 30.12.1997/1336. Kirjanpitolaki (The Finnish Accounting Act). The referenced Finnish version accessible at http://www.finlex.fi/fi/laki/ajantasa/1997/19971336?search%5Btype%5D=pika&search%5Bpika%5D=kirjanpitolaki

AIRMIC, ALARM & IRM. (2002). Risk Management Standard. London, 14 p. Accessible at http://www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf

AIRMIC, ALARM & IRM. (2010). Structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000. London, 18 p. Accessible at http://theirm.org/documents/SARM_FINAL.pdf

AON. (2010). Global Enterprise Risk Management Survey. Chicago, 53 p. Accessible at http://www.aon.com/attachments/2010_Global_ERM_Survey.pdf

COSO. (2004). Enterprise Risk Management – Integrated Framework, Executive Summary. Altamonte Springs, 7 p. Accessible at http://www.coso.org/documents/coso_erm_executivesummary.pdf

COSO. (2009). Strengthening Enterprise Risk Management for Strategic Advantage. Altamonte Springs, 20 p. Accessible at http://www.coso.org/documents/COSO_09_board_position_final102309PRINTandWEBFINAL_000.pdf

COSO. (2011). Embracing Enterprise Risk Management – Practical Approaches for Getting Started. Altamonte Springs, 14 p. Accessible at http://www.coso.org/documents/EmbracingERM-GettingStartedforWebPostingDec110_000.pdf

EU Corporate Governance Framework. (2011). The European Commission, Brussels, Green Paper, 23 p. Accessible at http://ec.europa.eu/internal_market/company/docs/modern/com2011-164_en.pdf

Fagg, S. (2007). In the loop: risk reporting. [web document]. Published 17.7.2007. Accessible at http://www.insurancebusinessonline.com.au/cri/article/in-the-loop-risk-reporting-126579.aspx

FERMA. (2003). Risk Management Standard. Federation of European Risk Management Associations, Brussels, 16 p. Accessible at http://www.ferma.eu/wp-content/uploads/2011/11/a-risk-management-standard-english-version.pdf

FIN-FSA Standard 5.1. (2009). Disclosure of periodic information - Regulations and guidelines. The Financial Supervisory Authority, Helsinki, standard, 69 p. Accessible at http://www.finanssivalvonta.fi/en/Regulation/Regulations/Financial_sector/5_Disclosure_of_information/Documents/5.1.std2.pdf

FIN-FSA Standard 5.2b. (2010). Disclosure obligation of the issuer and shareholder - Regulations and guidelines. The Financial Supervision Authority, Helsinki, standard, 46 p. Accessible at http://www.finanssivalvonta.fi/en/Regulation/Regulations/Financial_sector/5_Disclosure_of_information/Documents/5.2b.std6.pdf

Hume, S. (2010). Financial Reporting and Disclosure Risk Management, in the book: Fraser, J. & Simkins, B.J. (edit.), Enterprise risk management.

Today's leading research and best practices for tomorrow's executives. John Wiley & Sons, Inc., New Jersey, p. 369-384.

Ilmonen, I., Kallio, J., Koskinen, J. & Rajamäki, M. (2010). Johda riskejä – käytännön opas yrityksen riskienhallintaan. Tammi, Helsinki, 213 p.

Institute of Operational Risk. (2010). Operational Risk Sound Practice Guidance. Key Risk Indicators. London, 37 p. Accessible at https://subscriber.riskbusiness.com/ComponentFiles/Website/InterestingReading_Filename_95.pdf

ISO 31000 (2009). Risk management – Principles and guidelines. International Organization for Standardization, Geneva, standard, 24 p.

ISO/IEC Guide 73 (2009). Risk management – Vocabulary. International Organization for Standardization, Geneva, 13 p.

Kuusela, H. & Ollikainen R. (edit.). 2005. Riskit ja riskienhallinta. Tampere University Press, Tampere, 292 p.

Lam, J. & Associates. (2008). Emerging Best Practices in Developing Key Risk Indicators and ERM Reporting. Cognos, Burlington, 16 p. Accessible at ftp://ftp.software.ibm.com/software/data/sw-library/cognos/pdfs/whitepapers/wp_best_pract_in_dev_key_risk_indicators_erm_rep.pdf

NASDAQ OMX Helsinki. (2011). Harmonized Disclosure Rules. Helsinki, 21 p. Accessible at http://www.nasdaqomx.com/digitalAssets/75/75687_harmonized_disclosure_rules_fin_01092011_final.pdf

NASDAQ OMX Helsinki. (2013). Rules of the Stock Exchange. Helsinki, 47 p. Accessible at http://www.nasdaqomx.com/digitalAssets/83/83924_rulesofthestockexchange31january2013.pdf

OECD. (2004). Principles of Corporate Governance. Paris, 67 p. Accessible at

http://www.oecd.org/corporate/ca/corporategovernanceprinciples/31557724.pdf

Protiviti. (2010). Board Risk Oversight – A Progress Report. COSO, Menlo Park, 18 p. Accessible at http://www.coso.org/documents/Board-Risk-Oversight-Survey-COSO-Protiviti_000.pdf

PwC. (2012). Pillar 2 - Operational issues of risk management. PricewaterhouseCoopers International Limited, Paris, White Paper, 60 p. Accessible at http://www.pwc.com/en_GX/gx/insurance/solvency-ii/countdown/pdf/pwc-pillar-2-operational-issues-of-risk-management.pdf

Securities Market Association. (2010). Finnish Corporate Governance Code. Helsinki, 27 p. Accessible at http://cgfinland.fi/en/about-corporate-governance/corporate-governance-and-finnish-legislation/

Segal, S. (2011). Corporate Value of Enterprise Risk Management. The Next Step in Business Management. John Wiley & Sons, Inc., New Jersey, 404 p.