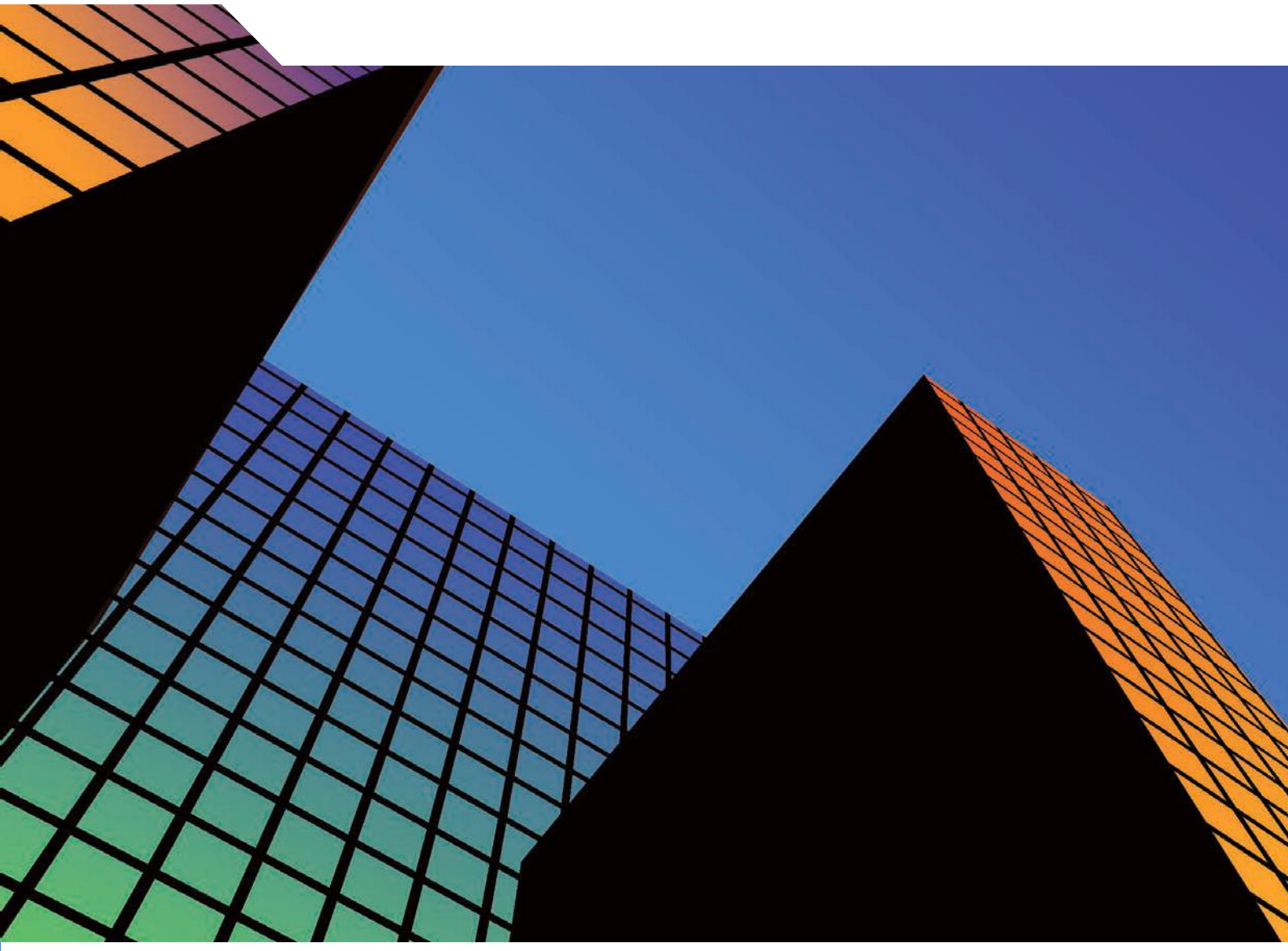
Corporate Governance

Risk Management and Corporate Governance



OECD

Corporate Governance

Risk Management and Corporate Governance

BETTER POLICIES FOR BETTER LIVES

Please cite this publication as:
OECD (2014), *Risk Management and Corporate Governance*, Corporate Governance, OECD Publishing.
http://dx.doi.org/10.1787/9789264208636-en

ISBN 978-92-64-20862-9 (print)
ISBN 978-92-64-20863-6 (PDF)

Series: Corporate Governance
ISSN 2077-6527 (print)
ISSN 2077-6535 (online)

Foreword

This report presents the results of the OECD's sixth peer review based on the OECD Principles of Corporate Governance. *The report reviews the corporate governance framework and practices relating to corporate risk management. It covers 27 jurisdictions.*

The report is based in part on a questionnaire that was sent to all participating jurisdictions in December 2012. In a second stage, the corporate governance framework and practices relating to corporate risk management in three jurisdictions (Norway, Singapore and Switzerland) were reviewed in more detail based upon a more focused set of questions and visits by the OECD Secretariat. The purpose of these case studies is to highlight national practices that may be of principal importance and particularly useful as a reference. The report was prepared by Winfrid Blaschke, Daniel Blume, Hans Christiansen and Akira Nozaki, and was conducted in co-operation with the OECD Working Party on State Ownership and Privatisation Practices (WP SOPP).

The OECD corporate governance peer review process is designed to facilitate effective implementation of the OECD Principles and to assist market participants, regulators and policy makers. It is carried out through an exchange of experiences and expertise that provides participants with an overview of existing practices and approaches and an opportunity to identify good practices that can stimulate and guide improvements. The reviews are also forward looking, so as to help identify key market practices and policy developments that may undermine the quality of corporate governance. The review process is open to OECD and non-OECD jurisdictions alike.

Table of contents

Tables

Figures

Executive summary

This report reviews the corporate governance framework and practices relating to corporate risk management in 27 of the jurisdictions that participate in the OECD Corporate Governance Committee. Against the background of the *OECD Principles of Corporate Governance*, it describes how various jurisdictions have chosen to implement the Principles relating to risk management.

The report analyses the corporate governance framework and practices relating to corporate risk management, in the private sector and in state-owned enterprises (SOEs). It is based upon a general survey of participating jurisdictions, complemented by three country studies illustrative of different aspects of risk management and corporate governance (Norway, Singapore and Switzerland).

The review finds that, while risk-taking is a fundamental driving force in business and entrepreneurship, the cost of risk management failures is still often underestimated, both externally and internally, including the cost in terms of management time needed to rectify the situation. Corporate governance should therefore ensure that risks are understood, managed, and, when appropriate, communicated.

Following the financial crisis, many companies have started to pay more attention to risk management. This is, however, seldom reflected in changes to formal procedures, except in the financial sector and in companies that have suffered serious risk management failure in the recent past. It appears that most companies consider that risk management should remain the responsibility of line managers.

Responding to public and/or shareholder pressures, some company boards, especially in widely-held companies, have started to review their incentive structures, including through the reduction of potential incentives for excessive risk-taking, notably stock options for top executives. Listed company boards need to be provided with incentive structures that appropriately reward business success, as well as awareness and management of risk.

Existing risk governance standards for listed companies still focus largely on internal control and audit functions, and primarily financial risk, rather than on (*ex ante*) identification and comprehensive management of risk. Corporate governance standards should place sufficient emphasis on *ex ante* identification of risks. Attention should be paid to both financial and non-financial risks, and risk management should encompass both strategic and operational risks.

Currently, risk governance standards tend to be very high-level, limiting their practical usefulness, and/or focus largely on financial institutions. There is scope to make risk governance standards more operational, without narrowing their flexibility to apply them to different companies and situations. Experiences from the financial sector can be

valuable, even if not necessarily transferable to the non-financial sector. Outsourcing- and supplier-related risks, for example, deserve attention in both the financial and the non-financial sector.

It is not always clear that boards place sufficient emphasis on potentially "catastrophic" risks, even if these do not appear very likely to materialise. More guidance may be provided on managing the risks that deserve particular attention, such as risks that will potentially have large negative impacts on investors, stakeholders, taxpayers, or the environment. Boards should be aware of the shortcomings of risk management models that rely on questionable probability assumptions.

SOEs should follow similar risk governance practices as listed enterprises, but this is often not formalised in implementable regulation. Deviations from listed company standards should be duly motivated, and not just be the result of lack of applicability of corporate governance codes. Sometimes, SOEs are subject to separate risk management oversight through sectoral regulators, whole-of-government risk management systems, or government audit institutions. Risk oversight at sub-federal level SOEs tends to be less developed and more uneven than at the federal level.

SOE board practices differ, with some countries considering risk as an issue for the whole board, others tasking the board audit committee with the work, and still others establishing risk committees. As in the private sector, these choices are often affected by factors such as size and sectors the SOE is operating in. Whichever structure is selected, effective oversight needs to be assured. Some countries mandate external auditors to review risk governance in SOEs.

For SOEs a crucial balance needs to be struck between controlling risk through direct action from the ownership function and through delegation to the board of directors. Some countries curtail SOE risk taking through top-down rules on activities and liabilities, while others place a high degree of reliance on boards and board committees. The state should ensure that, as part of the nomination process, the boards of directors have sufficient expertise to understand the risks incurred by the SOE. Without intervening in the day-to-day management of SOEs, the relevant ownership function should use all the opportunities it has, both in formulating strategic directives, and in its regular ownership dialogues, to ensure that the SOEs have proper risk management frameworks in place.

Chapter 1

Risk management governance framework and practices in 27 jurisdictions

This report presents the results of the OECD's sixth peer review based on the OECD Principles of Corporate Governance. *The report reviews the corporate governance framework and practices relating to corporate risk management in the private sector and in state-owned enterprises.*

Chapter 1 of the report summarises the corporate governance framework and practices relating to corporate risk management in 27 of the jurisdictions that participate in the OECD Corporate Governance Committee. It is based upon a questionnaire that was sent to all participating jurisdictions in December 2012, discussions in the OECD Corporate Governance Committee in April and November 2013, as well as conclusions from the three in-depth studies of the corporate governance framework and practices relating to corporate risk management in Norway, Singapore and Switzerland contained in Chapters 2-4.

The statistical data for Israel are supplied by and under the responsibility of the relevant Israeli authorities. The use of such data by the OECD is without prejudice to the status of the Golan Heights, East Jerusalem and Israeli settlements in the West Bank under the terms of international law.

1.1. Background to the review

Risk management failures at major corporations have captured the headlines for many years, primarily in the financial sector, but in other sectors as well, and have not always been the result of shortcomings in financial risk-taking. Environmental catastrophes such as Deep Water Horizon or Fukushima come to mind (or, less recently, Bhopal and Seveso), as well as accounting fraud (e.g. Olympus, Enron, WorldCom, Satyam, Parmalat), or foreign bribery (e.g. Siemens) cases, to name just a few from the non-financial sector. Often these failures were (at least) facilitated by corporate governance failures, where boards did not fully appreciate the risks that the companies were taking (if they were not engaging in reckless risk-taking themselves), and/or deficient risk management systems.

The importance of an effective risk governance framework was underlined in the Committee's report from 2009 on *The Corporate Governance Lessons from the Financial Crisis*. The present review complements the Committee's 2009/10 reviews with a survey of member and partner jurisdictions participating in the Corporate Governance Committee, with a view toward drawing lessons about the adequacy of existing corporate governance principles, guidelines, and practices in this area.

Risk governance has also been addressed in the Committee's thematic reviews following the financial crisis, notably in the review on board practices, where the Committee examined incentives influencing corporate risk-taking, notably with regard to compensation practices (OECD, 2011). The issue has also been dealt with by the OECD's Asian and Latin American Corporate Governance Roundtables. The Financial Stability Board (FSB), in its recently issued *Thematic Review on Risk Governance*, called on the OECD to review its principles for governance, taking into consideration the sound risk governance practices listed in the FSB report and reproduced in Annex A to this report (Financial Stability Board, 2013).

The present review covers 22 OECD member countries, together with **Argentina**; **Hong Kong**, **China**; **India**; **Lithuania** and **Singapore**. A general overview of risk governance practices in all participating jurisdictions is provided. A more detailed review of three jurisdictions (**Norway**, **Singapore** and **Switzerland**) was carried out in order to highlight either particular aspects of the risk governance framework, or country specific circumstances that may influence the choice of approach.

1.2. Scope of the review

The review addresses the issue of risk management from the perspective of corporate governance ("risk governance") based upon the relevant *OECD Principles of Corporate Governance* (hereafter "the Principles"). In order to avoid, as much as possible, overlap with similar reviews conducted by other organisations such as the recently completed thematic peer review of risk governance by the Financial Stability Board and the 2010 Principles for Enhancing Corporate Governance of the Basel Committee on Banking Supervision (in both of which the OECD Secretariat actively participated), this review focuses on risk

governance issues that are relevant for companies in all sectors (including state-owned), rather than those concerning primarily financial intermediaries.

Included in this review is a chapter on the risk management practices of state-owned enterprises, whose risk management failures are likely to have an impact, directly or indirectly, on government finances. Examples abound of major risk management failures in and outside the financial sector, many of them attributed to a lack of risk oversight by boards of state-owned enterprises. The direct cost to taxpayers of these failures has been enormous.

1.3. The perspective of the OECD Principles and Guidelines

The starting point for this review is Principle VI.D., which states that the board should fulfil certain key functions, including reviewing and guiding corporate risk policy as well as ensuring that appropriate systems for risk management are in place and comply with the law and relevant standards. The Annotations to the Principles add that *boards have an essential responsibility setting the risk policy by specifying the types and degree of risk that a company is willing to accept in pursuit of its goals*.

Complementary to this, the annotations to Principle VI.D.7 note that "ensuring the integrity of the essential reporting and monitoring systems will require the board to set and enforce clear lines of responsibility and accountability throughout the organisation". The annotations further elaborate that the board will also need to ensure that there is appropriate oversight by senior management.

Chapter V.E of the *OECD Guidelines on Corporate Governance of State-Owned Enterprises* (hereafter "the Guidelines") stipulates that SOEs should disclose material information on all matters described in the *OECD Principles of Corporate Governance* and in addition focus on areas of significant concern for the state as an owner and the general public. Material risk factors and measures taken to manage such risks are one example of such information specifically mentioned in the Guidelines (see Box 1.1).

Box 1.1. **Risk transparency and disclosure in the SOE Guidelines**

The Annotations to the *OECD Guidelines on Corporate Governance of State-Owned Enterprises* explicitly highlight risk governance issues for SOEs. Chapter V.E.3 notes the following:

Severe difficulties arise when SOEs undertake ambitious strategies without clearly identifying, assessing or duly reporting on the related risks. Disclosure of material risk factors is particularly important when SOEs operate in newly de-regulated and increasingly internationalised industries where they are facing a series of new risks, such as political, operational, or exchange rate risks. Without adequate reporting of material risk factors, SOEs may give a false representation of their financial situation and overall performance. This in turn may lead to inappropriate strategic decisions and unexpected financial losses.

Appropriate disclosure by SOEs of the nature and extent of risk incurred in their operations requires the establishment of sound internal risk management systems to identify, manage, control and report on risks. SOEs should report according to new and evolving standards and disclose all off-balance-sheet assets and liabilities. When appropriate, such reporting could cover risk management strategies as well as systems put in place to implement them. Companies in extracting industries should disclose their reserves according to best practices in this regard, as this may be a key element of their value and risk profile.

Box 1.1. **Risk transparency and disclosure in the SOE Guidelines** *(cont.)*

Public Private Partnerships should also be adequately disclosed. Such ventures are often characterised by transfers of risks, resources and rewards between public and private partners for the provision of public services or public infrastructure and may consequently induce new and specific material risks.[*]

[*] See also *OECD Principles for Public Governance of Public-Private Partnerships* (*www.oecd.org/governance/oecdprinciplesforpublicgovernanceofpublic-privatepartnerships.htm*).

Chapter VI.E of the *Guidelines* further stipulates that, when necessary, SOE boards should set up specialised committees to support the full board in performing its functions, particularly in respect of audit, risk management and remuneration. The annotations further note that the setting up of specialised board committees could be instrumental in reinforcing the competency of SOE boards and in underpinning their critical responsibility in matters such as risk management and audit.

1.4. Corporate governance and the financial crisis

The OECD Corporate Governance Committee already completed several papers on risk management in the context of its work on *Corporate Governance and the Financial Crisis* during 2009-10. Since then, additional work has been conducted in various fora (including the Financial Stability Board), to a large degree focused on financial institutions, and boards are reported to have increased their focus on risk in the last few years. Overall, however, the conclusions from the OECD's 2010 review, which are summarised in Box 1.2, appear to be still valid.

Box 1.2. **Corporate Governance and the Financial Crisis (OECD, 2010) Key findings and main messages: Effective implementation of risk management**

- Perhaps one of the greatest shocks from the financial crisis has been the widespread failure of risk management. In many cases risk was not managed on an enterprise basis and not adjusted to corporate strategy. Risk managers were often separated from management and not regarded as an essential part of implementing the company's strategy. Most important of all, boards were in a number of cases ignorant of the risk facing the company.
- It should be fully understood by regulators and other standard setters that effective risk management is not about eliminating risk taking, which is a fundamental driving force in business and entrepreneurship. The aim is to ensure that risks are understood, managed and, when appropriate, communicated.
- Effective implementation of risk management requires an enterprise-wide approach rather than treating each business unit individually. It should be considered good practice to involve the board in both establishing and overseeing the risk management structure.
- The board should also review and provide guidance about the alignment of corporate strategy with risk-appetite and the internal risk management structure.
- To assist the board in its work, it should also be considered good practice that risk management and control functions be independent of profit centres and the "chief risk officer" or equivalent should report directly to the board of directors along the lines

Box 1.2. **Corporate Governance and the Financial Crisis (OECD, 2010) Key findings and main messages: Effective implementation of risk management** *(cont.)*

already advocated in the OECD Principles for internal control functions reporting to the audit committee or equivalent.

- The process of risk management and the results of risk assessments should be appropriately disclosed. Without revealing any trade secrets, the board should make sure that the firm communicates to the market material risk factors in a transparent and understandable fashion. Disclosure of risk factors should be focused on those identified as more relevant and/or should rank material risk factors in order of importance on the basis of a qualitative selection whose criteria should also be disclosed.
- With few exceptions, risk management is typically not covered, or is insufficiently covered, by existing corporate governance standards or codes. Corporate governance standard setters should be encouraged to include or improve references to risk management in order to raise awareness and improve implementation.

Source: OECD (2010), *Corporate Governance and the Financial Crisis – Conclusions and Emerging Good Practices to Enhance Implementation of the Principles*, OECD, Paris, *www.oecd.org/daf/ca/corporategovernanceprinciples/44679170.pdf*.

As the 2009/10 review noted, the financial crisis uncovered extremely deficient risk oversight and management practices even at highly sophisticated corporations. In many cases, risk was not managed on an enterprise wide basis and not adjusted to corporate strategy, as risk managers were often kept separate from management and not regarded as an essential part of implementing the company's strategy. Moreover, boards were in a significant number of cases ignorant of the risk facing the company.

Since the beginning of the financial crisis, various surveys have revealed that corporations developing their risk management and oversight practices still face challenges, such as linking risks to strategy; better defining risks; developing corporate responses to risks that manage to address all five key dimensions (strategy, people, detail, tasks, and drivers); effectively considering stakeholders' and gatekeepers' concerns; and addressing all these issues from a whole-enterprise perspective. These challenges are faced by both financial and non-financial companies.

1.5. Risk management practices in listed companies

General perspective

As noted above, effective risk management is not about eliminating risk taking, which is indeed a fundamental driving force in business and entrepreneurship. At the same time, the need to strengthen risk management practices has been one of the main lessons from the financial crisis, for both financial and non-financial companies. While this is well recognised, there is limited evidence that listed companies have in fact paid significantly more attention to risk management in recent years. For example, in a 2011 survey by McKinsey, 44% of respondents said that their boards simply review and approve management's proposed strategies. The same survey found that only 14% of board time was spent on business risk management, and that 14% of respondents had a complete understanding of the risks their company faced. Half of directors said that the information they received was too short-term.

The risks that companies face are both financial and non-financial. In the context of financial institutions, the focus naturally tends to be on financial risks, such as credit, liquidity or market risks, although there is also an increasing emphasis on operational risk. In the case of non-financial institutions, the same risks will also be present, although not always to the same extent as in financial institutions. Other risks, such as IT and outsourcing risks are likely to concern non-financial institutions just as much, and in some cases (environmental, safety and health risks) are of stronger primary concern to non-financial corporations. Risk governance rules and practices appropriate for financial institutions therefore may not be directly applicable to non-financial institutions. At the same time, some more general lessons can probably be learned from risk management failures in the financial sector.

Since the beginning of the financial crisis, many reports have focused on risk governance in financial institutions, including major reports by the Basel Committee on Banking Supervision, the Group of Thirty, the Institute of International Finance, and others. The most recent report has been the Financial Stability Board's Thematic Peer Review on Risk Governance, which is summarised in Box 1.3. (A list of "sound risk governance principles" drafted by the FSB is also attached as Annex A). Relatively little work has been done, however, on risk governance in the non-financial sector, notably with regard to the lessons to be learned from risk management failures more generally.

Box 1.3. **Financial Stability Board Thematic Peer Review on Risk Governance (2013)**

The Financial Stability Board's Thematic Peer Review on Risk Governance takes stock of risk governance practices at both national authorities and firms, notes progress made since the financial crisis, identifies sound practices and offers recommendations to support further improvements.

The recent global financial crisis exposed a number of risk governance weaknesses in major financial institutions, relating to the roles and responsibilities of corporate boards of directors (the "board"), the firm-wide risk management function, and the independent assessment of risk governance. Without the appropriate checks and balances provided by the board and these functions, a culture of excessive risk-taking and leverage was allowed to permeate in many of these firms.

The peer review found that, since the crisis, national authorities have taken several measures to improve regulatory and supervisory oversight of risk governance at financial institutions. These measures include developing or strengthening existing regulation or guidance, raising supervisory expectations for the risk management function, engaging more frequently with the board and management, and assessing the accuracy and usefulness of the information provided to the board to enable effective discharge of their responsibilities. Nonetheless, more work is necessary. In particular, national authorities need to better assess the effectiveness of a firm's risk governance framework, and more specifically its risk culture, to help ensure the sound management of risk through the economic cycle. Supervisors will need to strengthen their assessment of risk governance frameworks to encompass an integrated view across all aspects of the framework.

The peer review also surveyed 36 banks and broker-dealers that FSB members deemed as significant for the purpose of the review. The evaluation of their responses indicates that many of the best risk governance practices at surveyed firms are now more advanced

Box 1.3. **Financial Stability Board Thematic Peer Review on Risk Governance (2013)** *(cont.)*

than national supervisory guidance, an outcome that may have been motivated by firms' need to regain market confidence. Despite these considerable strides, significant gaps remain in a number of areas, particularly in the risk management function. At the core of strong risk management is an effective risk appetite framework, and firms' progress to date is uneven in its development, comprehensiveness and implementation. Very few firms were able to identify clear examples of how they used their risk appetite framework in strategic decision-making processes.

Drawing from the findings of the review, the report identifies a list of sound risk governance practices (see Annex A to this report) that would help firms continue to improve their risk governance and national authorities to assess its effectiveness. The review also sets out several recommendations targeting areas where more substantial work is needed, in particular:

1. National authorities should strengthen their regulatory and supervisory guidance for financial institutions and devote adequate resources to assess the effectiveness of risk governance frameworks.
2. Standard setting bodies should review their principles for governance, taking into consideration the sound risk governance practices set out in the report.
3. The FSB should explore ways to formally assess risk culture at financial institutions.
4. The FSB should provide general guidance on the key elements that should be included in risk appetite frameworks and establish a common nomenclature for terms used in risk appetite statements.

Source: Financial Stability Board (FSB) (2013), *Thematic Review on Risk Governance*, *www.financialstabilityboard.org/publications/r_130212.pdf*.

The following sections highlight the main results from the questionnaire responses, notably in the areas of: 1) risk management standards and codes; 2) risk appetite and incentives; 3) chief risk officers; 4) board member qualification requirements; and 5) board committees. Section 1.6 then summarises the questionnaire responses relating to state-owned enterprises.

Risk management standards and codes

In many jurisdictions, risk management issues are dealt with (in one way or another) in national corporate governance codes, as is the case with the New York Stock Exchange (NYSE) listed company rules, the UK's combined code and the French AFEP-MEDEF code. Internationally, professional institutes and associations also offer their advice. In 1992, the Committee of Sponsoring Organisations of the Treadway Commission (COSO) published an internal control – integrated framework guide,[1] and in 2004 an enterprise risk management (ERM) – integrated framework guide.[2] A report prepared for the OECD in 2010 concluded, however, "none of the existing guidance on risk management is adequate for the purpose. Most of the guidance is extremely high-level, is process-oriented and gives scant guidance how to create an effective risk management and assurance framework."[3]

More recently, COSO published guidance on risk assessments and on risk appetite (2012), which provides more specific guidance on certain issues. In 2009, the International Organisation for Standardisation issued its standard for implementation of risk management

principles, ISO 31000, which has *de facto* become the world standard. The purpose of ISO 31000 is to provide principles and generic guidelines on risk management that could achieve convergence from a variety of standards, methodologies and procedures that differ between industries, subject matters, and countries.

The answers to the questionnaire for this review similarly highlight the inclusion of references to risk management in corporate governance codes (which in many countries operate on a comply-or-explain basis). Depending upon jurisdiction, references to risk management are also contained in listing rules or agreements (**India**, **UK**, and **US**), company laws (**Austria**, **Germany,**[4] **Turkey** and **Japan**), or stock exchange laws (**Mexico**), usually in connection with the audit or internal control functions. Additional guidance that is sometimes provided, such as the **UK**'s "*Turnbull Guidance*", also mainly refers to audit and internal controls. One exception is **Singapore**'s Corporate Governance Council, which in May 2012 issued guidance specifically on the governance of risk management ("*Risk Governance Guidance for Listed Boards*").[5]

Risk appetite and incentives

Whereas it is generally accepted that boards should be responsible for setting a company's risk appetite or tolerance, little guidance is available on how boards can go about setting risk targets, considering the various types of risks that modern corporations may be subject to. Aggregating all the risks into one number appears impossible, and even the existing models for aggregating financial risks (only) have largely been discredited during the financial crisis. Therefore, the only realistic option appears to be for boards to set risk appetite or tolerance with regard to each individual risk identified. At the same time, boards need to be aware of the possible interaction of different risk, notably the possibilities that they may reinforce each other.

An important conclusion from the Committee's 2010 report on *Corporate Governance and the Financial Crisis* was that the board's responsibility for defining strategy and risk appetite needs to be extended to establishing and overseeing enterprise-wide risk management systems. The report noted that in some important cases the risk management system was not compatible with a company's strategy and risk appetite. Judging from the results of the present survey, there appear to be, at the national level, few rules regarding the risk appetite of (non-financial) companies. Board responsibilities do not generally extend to ensuring that the risk management system is compatible with company strategy and risk appetite. An exception is **Singapore**'s Guidance, which specifically refers to financial, operational, compliance, information technology, and risk management systems.

In the context of the present survey, only **Germany** and **India** highlighted special provisions for major risks threatening the existence of the company. **Germany**'s stock company act requires the management board to introduce appropriate measures, in particular setting up a monitoring system, to ensure that any developments endangering the continued existence of the company may be identified and communicated to the management board early on. **India**'s companies act requires, in the context of a statement on risk management, the identification of risk which may threaten the existence of the company. While it is not clear how effective such rules have been in practice, the absence of such rules in most jurisdictions suggests that the focus of risk management may often be more on the risks considered most likely to materialise rather than on those having the largest potential impact, even if considered unlikely to materialise.[6]

Chief risk officer

Among the countries that responded to the survey, **Argentina** and **Singapore** referred to guidance documents that suggest the appointment of a chief risk officer in certain cases, and **India** reported that a rule requiring large listed companies to have a chief risk officer/manager is under consideration.[7] Where (usually larger or financial sector) corporations have decided to appoint a chief risk officer, the trend is that the risk management function is separate from profit centres and, primarily in the financial sector, reports directly to the board, notably to non-executive directors. How sufficient such arrangements are in practice, depends upon many factors, most importantly perhaps the company's overall risk culture. The financial crisis certainly did not provide assurance that chief risk officers were effectively able to restrain excessive risk-taking.

> "From the standpoint of an institution, the existence of a risk manager has less to do with actual risk reduction than it has to do with the impression of risk reduction" (Taleb, 2004).

In the financial sector, supervisors have therefore in many cases insisted that chief risk officer functions be upgraded, made more independent, better-resourced, and involved in decision-making. Whereas such sound risk governance practices for financial institutions will not be applicable or necessary for all types of companies, some may make sense also for larger companies, and/or those operating in high-risk sectors. The FSB, for example, considered it sound practice for risk management functions (at financial institutions), to have access to relevant affiliates, subsidiaries, and concise and complete risk information on a consolidated basis; for risk-bearing affiliates and subsidiaries to be captured by the firm-wide risk management system and be a part of the overall risk governance framework (Financial Stability Board, 2013).

Qualification requirements

Qualification requirements for board members typically apply only for financial institutions and in many countries also for members of audit committees. The EU's Statutory Audit Directive (2006/43/EC) for example states that "a natural person may be approved to carry out a statutory audit only after having attained university entrance or equivalent level, then completed a course of theoretical instruction, undergone practical training and passed an examination of professional competence of university final or equivalent examination level, organised or recognised by the member state concerned". The Directive further requires that the test of theoretical knowledge cover the issues of risk management and internal control.

Some countries participating in the survey noted that new board members are offered training or participate in induction processes. It is unclear how far such programmes are able to transmit a sufficient degree of knowledge about risk management. They may help, but are unlikely to fully replace the knowledge that is gained through long-term industry experience.

Board committees

Typically, the risk management function within the board is found within the audit committee, reflecting common practice and/or legislative requirements. The EU's Statutory Audit Directive requires audit committees to monitor the effectiveness of the company's internal control, internal audit where applicable, and risk management systems, and

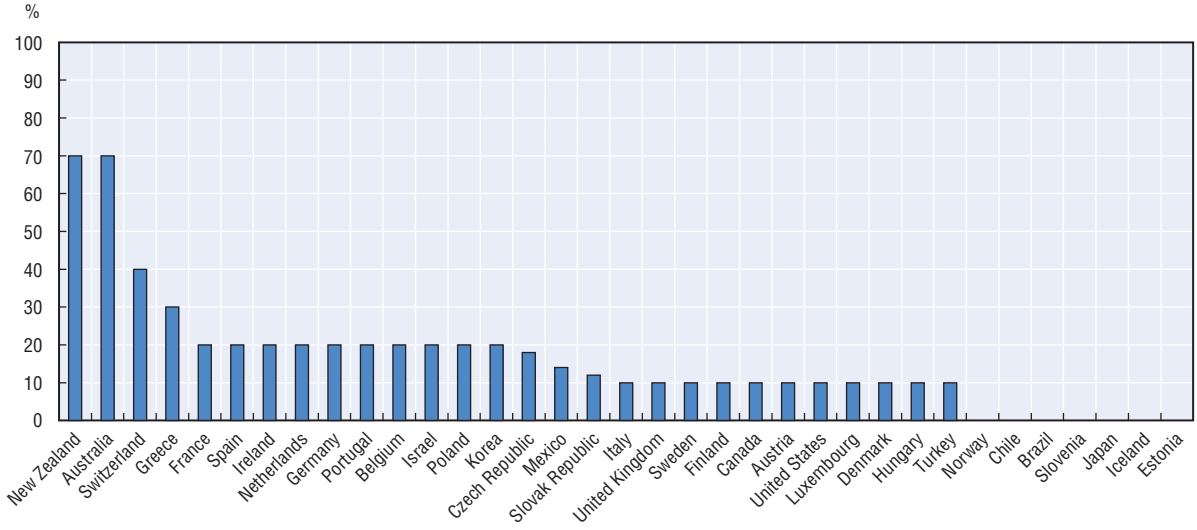
similar rules exist around the world. In the **US**, for example, the New York Stock Exchange (NYSE) listed company rules, as they stand, require audit committees to discuss policies with respect to risk assessment and risk management.[8] The FSB considers it to be "sound risk governance practice" that financial institutions have a stand-alone risk committee, distinct from the audit committee, has a chair who is an independent director and avoids "dual-hatting" with the chair of the board or any other committee.

The NYSE rules further comment that "while it is the job of the CEO and senior management to assess and manage the listed company's exposure to risk, the audit committee must discuss guidelines and policies to govern the process by which this is handled. The audit committee should discuss the listed company's major financial risk exposures and the steps management has taken to monitor and control such exposures. The audit committee is not required to be the sole body responsible for risk assessment and management, but, as stated above, the committee must discuss guidelines and policies to govern the process by which risk assessment and management is undertaken. Many companies, particularly financial companies, manage and assess their risk through mechanisms other than the audit committee. The processes these companies have in place should be reviewed in a general manner by the audit committee, but they need not be replaced by the audit committee."

In the survey, **Sweden** observed that audit committees are more active reviewing risk management systems, but that there was little evidence of follow-up. The challenge with such arrangements is typically to have the committee focus on explicit separate management of corporate risks as opposed to financial control. One of the conclusions from the Committee's work after the onset of the financial crisis was that frequently the focus appeared to have been on internal controls for the purpose of financial reporting, so that risk management became divorced from corporate strategy and its implementation.

A 2010 top-level survey of incentives and risk management at listed companies across OECD countries and Brazil conducted for the OECD by Manifest Information Services revealed a low incidence of specialised board committees to deal with risk (Figure 1.1). In contrast to remuneration, the issue of risk management is much less commonly stipulated

Figure 1.1. **Companies with a committee with explicit reference to risk (2010)**



Source: Manifest information Services (2010), *Board Practices: Incentives and Managing Risks – United Kingdom, Sweden, Portugal, Brazil and Japan*, Report commissioned by the OECD (unpublished).

Table 1.1. **Risk governance requirements/recommendations for listed companies**

	Board responsibilities	Board-level committee		Internal control/risk management system	Chief risk officers
		Audit	Risk		
Argentina	C	L/R	C	C	C
Australia					
Austria	L/C	L*/C*	-	L	-
Belgium					
Brazil					
Canada					
Chile	-	R	R	R	-
Czech Republic	-	-	-	-	-
Denmark					
Estonia					
Finland	-	C*	-	C	-
France					
Germany	L/C	L/C	-	L/C	-
Greece					
Hong Kong, China	R/C	C*	-	C	-
Hungary					
Iceland					
India	L/C	L*/C*	-	L/C	-
Indonesia					
Ireland					
Israel	-	L*	-	R	L*
Italy	C	L	C	C	C*
Japan	L	-	-	L	-
Korea	C	-	-	-	-
Lithuania	-	C*	-	-	-
Luxembourg					
Mexico	L	L	-	-	-
Netherlands	C	C*	-	C	-
New Zealand	-	-	-	-	-
Norway	C	L*	-	L/C	-
Poland	-	L*	-	L	-
Portugal	-	-	-	-	-
Saudi Arabia					
Singapore	C	C	C	C	C
Slovak Republic					
Slovenia	-	C*	-	C	-
Spain	-	L*/C*	-	L/C	-
Sweden	C	-	-	C	-
Switzerland	L	C*	-	C	-
Turkey	R	L	L	L	-
United Kingdom	C	C*	-	C	-
United States	R*	L*/R*	-	L/R	-

Notes: "**L/R/C**" denote laws, regulations, and codes or principles respectively. "**-**" denotes the absence of a specific requirement or recommendation (outside the financial sector).
Board responsibilities: Specific provisions describing the board responsibilities for risk management. * In the US, the SEC rules require a company to disclose the board's role in the oversight of risk. **Board-level committee:** Requirement or recommendation regarding the establishment of a board-level committee charged with risk management.
* denotes that risk management is explicitly included in the role of audit committee. **Internal control/risk management system:** Requirement or recommendation regarding implementation of the internal control and risk management system. **Chief risk officers:** Requirement or recommendation regarding a chief risk officer. * denotes that internal auditors are in charge of risk management.
Source: Country responses to OECD peer review questionnaire.

by company law or best practice code as needing or requiring a separate committee in order to address it. Consequently, few companies in that survey had a committee whose title included any reference to risk management.

While some countries (e.g. **UK**) pointed to an increasing trend toward the creation of board-level risk committees in large companies, the present survey revealed that few countries have any explicit rules or recommendation or guidance on risk committees outside the financial sector. **India** and **Singapore** have, however, issued guidance on risk committees, **Italy**'s corporate governance Code refers to a "Control and Risk Committee", and **Turkey**'s commercial Code requires companies to set up a "Committee for the Early Identification of Risks". **Poland** noted that some state-owned enterprises have risk committees, and **Sweden** observed that energy companies tend to have risk committees.

The responsibility for establishing and overseeing the company's enterprise-wide risk management system usually rests with the board of directors as a whole. In most cases, this responsibility is stated in company law and/or listing rules, except in a small number of jurisdictions where this is not clearly stated. In some jurisdictions, including the **US (NYSE**[9]**)**, the responsibility rests with the audit committee. **Switzerland** recently abolished, due (among other things) to proportionality concerns for smaller companies, the requirement that risk management systems be reviewed by external auditors, and the **UK**'s Financial Reporting Council argues against mandating external auditor reviews of risk management systems.

1.6. Risk management practices in state-owned enterprises

When assessing risk-taking behaviour in the recent financial crisis, two types of institutions have stood out: i) state-owned financial institutions considered as SOEs; and ii) enterprises owned by the sub-national levels of government considered as SOEs.[10] Some of the most problematic examples of risk management failure occurred in banks and other financial institutions owned by sub-national levels of government. Many such financial institutions have in fact suffered significantly larger losses than comparable private entities. One possible reason may be that their risk governance was of lower quality. Other explanations put forward in recent years are that boards of directors may have been of a lower quality than in the private sector and/or that the state did not exercise its ownership function properly.

SOEs versus listed companies

Almost all jurisdictions responded that there are no material differences between risk governance practices in non-listed SOEs and listed companies. This is despite the fact that, in many cases, this is not a requirement emanating from the legal or regulatory frameworks. What appears to underlie the responses is an issue of company size: some SOEs are very large, but most are small and have specific purposes. Governments therefore do not wish to mandate that all SOEs operate according to listed standards, but they expect their particularly large or particularly commercially-oriented SOEs to do so. Likewise, state-owned financial institutions are normally expected – regardless of size – to operate according to similar risk management practices as listed private entities (although, as mentioned above, this expectation has not always been met).

In terms of whether SOEs are held up to the standards of listed companies, the respondents fall into three main categories. One group of countries, sometimes noting that

there is no framework to ensure that non-listed SOEs comply with certain risk governance standards, made no mention of legal or regulatory requirements of the kind concerned (**Austria**; **Czech Republic**; **Germany**; **Hong Kong**, **China**; **Korea**; **Mexico**; **New Zealand**; **Poland**; **Spain** and **Turkey**). However, several of these noted that in practice (large) unlisted SOEs do have risk management practices that differ little from those of listed companies. At the opposite extreme, the Korean response indicated that "there surely are material differences between risk governance practices in unlisted SOEs and listed companies", effectively arguing that risk management may be stronger in SOEs. Listed companies in **Korea**, it is argued, rely on their own internal governance and corporate culture for risk management, whereas there are externally mandated risk management frameworks in place in the SOEs.

A second group does require non-listed SOEs to comply with the same risk governance standards as listed companies (**Finland**[11], **Italy** and **Sweden**). A third group of jurisdictions (**Argentina**, **Chile**, **India**[12], **Israel**, **Japan**, **Lithuania**, **Norway**, **Portugal** and **Switzerland**) set out specific standards for SOEs, but equivalence or mutual relationship between these standards and those for listed companies can hardly be assessed. One country (the **Netherlands**) makes it optional for SOEs whether to comply with listed company governance codes on a comply-or-explain basis.

Finally, a few countries (e.g. **Argentina**) observed that risk management is generally not well developed in SOEs. This may have to do with the way SOEs are perceived and positioned within the public sector. Other things equal one might expect that the more strongly a country's SOEs are corporatised the more fully will they have embraced private sector best practices in respect of risk management. The Mexican response (Box 1.4) provides an example of a risk management culture that is particularly reliant on the involvement of the general government sector, and of the CEO as opposed to the board of directors.

Box 1.4. **Mexican guidelines for internal control of SOEs**

The "General Guidelines for Internal Control" issued by the Mexican Ministry of Public Governance provide that central government agencies shall have a Control and Institutional Performance Committee responsible for, among others, risk detection and management. The establishment of these committees in the case of SOEs is optional, since they are not considered, in *strictu sensu*, as government agencies.

However, the General Guidelines provide the mandatory creation in all SOEs, and under the direction of the CEO, of an Internal Institutional Control System, which allows the implementation of a systematic process to identify, assess, prioritise, manage and monitor the risks that may impede or prevent compliance with institutional goals and objectives, analysing internal and external factors that may increase the impact and likelihood of risks materialising, and defining strategies and actions to control them. This, by establishing and updating policies, procedures, mechanisms and actions required to manage risks, reasonably achieve institutional goals and objectives and comply with regulations applicable to public management.

The System's implementation begins with an annual self-assessment, whose results allow the establishment of a Risk Management methodology, which takes place in three stages: i) risk assessment; ii) assessment of controls; and iii) final assessment of risks relative to controls. The methodology produces the following:

1. *Institutional Risk Map*. Allows prioritisation of risks based on their probability of occurrence and degree of impact.

Box 1.4. **Mexican guidelines for internal control of SOEs** *(cont.)*

2. *Strategies and Actions for risk administration*. The strategies are the options for managing the risk based on their assessment relative to controls in order to avoid, reduce, assume or transfer the risk, as a result of these actions, mechanisms are put in place for implementing the strategies, most relevant are optimisation of policies, programs, projects, processes, procedures and services, among others.

These documents, among others, and their updates, are presented at least annually to the board of directors. Risk management is under the direct responsibility of the CEO, who is aided by a Coordinator for Internal Control, responsible for submitting to the CEO's approval the risk management methodology and policies, as well as actions to implement them.

Source: Mexican response to OECD peer review questionnaire.

Risk appetite and incentives

Regarding managerial incentives, the respondents broadly agreed on the position that the variable element of managerial remuneration in SOEs is so relatively limited that it does not encourage managers to take excessive risk. Among the countries making specific reference to remuneration guidelines and practices to dis-incentivise excessive risk taking were the **Czech Republic, Norway** and **Switzerland**. The **Netherlands** informed that it is reconsidering the existing requirement that SOE board members receive variable remuneration.

As for mechanisms to limit risk taking, they fall into two broad categories, namely: i) those that affect the general financial and operating environment of SOEs; and ii) guidelines and instructions regarding the daily management of companies. In the first category, the approaches reported by various respondents in turn depend on the degree of corporatisation of SOEs and closeness between the SOEs and the general government sectors. In general, four overall approaches can be discerned:

- *Direct control*. Governments still exercise direct control over major transactions by SOEs, which may of course serve as the ultimate control instrument. In many jurisdictions this may be limited to large-scale acquisition and disposal of assets, but some governments go further. The **Indian** response indicates this as an important risk management tool.[13]
- *Approval of SOE liabilities*. The most commonly cited way of controlling (financial) risk is the fact that SOEs in most jurisdictions are subject to an approvals procedure – typically involving the Ministry of Finance – if they wish to materially increase their liabilities. Among the respondents listing this as a risk limitation tool were **Chile**, **Japan**, **Mexico** and the **Netherlands**.
- *Extent of guarantees*. Most SOEs operate without government guarantees (although markets may in practice often perceive implicit guarantees), but those that are tasked with public policy objectives may still be explicitly state-backed. Some respondents (e.g. **Chile**, **Germany**, **Israel** and **New Zealand**[14]) list the explicit limitation of the extent of such guarantees as another risk control tool.
- *Sectoral regulation or legislation*. In some countries the scope of activities that any given SOE may engage in is stipulated in statutory rules or regulation. The responses from **Japan** and **Mexico** identify (for some sectors) this as a risk management tool.

At the same time, it must be recognised that, in many jurisdictions, the risk-taking of SOEs is considered mostly as an issue for the generally on-going surveillance by the

government (often the Ministry of Finance). In most cases, this surveillance consists, however, to a large extent of quarterly or semi-annual reporting of financial results, in some cases supplemented by disclosure of risk assessments. As the financial crisis has demonstrated, such *ex post* reporting may frequently come too late to alert boards to excessive risk-taking. The same reservation applies to the widespread reliance on state audit bodies to monitor risk (in individual SOEs as well as the ownership function) to which many questionnaire responses made reference.

As noted earlier, a number of ownership functions or (other) ministries have issued guidelines on risk taking and risk managements to their SOEs. The arrangements can be more or less formal. The **New Zealand** response notes that the state "like any other shareholder, from time to time indicates its risk tolerance to the boards it appoints". Where formal guidelines exist they may be either a stand-alone instrument, or imbedded in general governance codes for the SOE sector. In many cases, they cover both the risk management expectations to the companies and the specific responsibilities of the boards of directors (discussed in the following sub-section). One example of such guidelines was reported by **Israel**; it is reproduced in Box 1.5.

Box 1.5. **Israeli ownership circular on risk management in SOEs**

According to a circular published in 2009 by the Government Companies Authority (ownership unit), all SOEs are required to establish a risk management policy and supervise its implementation. The control mechanisms include the following:

a) The board is responsible to establish and approve the risk management policy and to supervise its implementation. Including, by means of internal reporting rules in the SOE approved by the board, the supervision of the board includes reviewing the performance of risk management, risks definition and grading, the organisation's functions and infrastructures, etc.

b) The board can appoint a special committee designated to risk management function or perform this function itself.

c) The SOE is required to appoint a designated management member responsible for risk management functions. In smaller SOEs (classified 6 or less), the board can decide that this function will be performed by outsourcing the services.

d) Risk management of the SOE is part of the company's internal auditor yearly plan.

Source: Israeli response to OECD peer review questionnaire.

Other examples include **Lithuania**, where the Ministries of Finance and Economy issued financial risk management guidelines in 2012, detailing principles concerning: i) the management of SOE funds held with commercial banks; ii) investment strategies for SOE financial assets; iii) derivatives transactions. **India** (whose board-related practices are reported in Box 1.6) reports that SOEs are subject to stricter monitoring than listed companies with respect to risk taking, inter alia due to monitoring by a Central Vigilance Commission. The questionnaire response opines that this might actually contribute to disincentives to SOE risk-taking, making SOEs excessively risk-averse.

Box 1.6. **India – Risk management in the Guidelines on Corporate Governance for Central Public Sector Enterprises (DPE, 2010)**

Section 7.3 of the Guidelines, which are established under the auspices of the Department of Public Enterprises (DPE) and mandatory for Indian SOEs, makes the following stipulations:

The company shall lay down procedures to inform board members about the risk assessment and minimisation procedures. These procedures shall be periodically reviewed to ensure that executive management controls risk through means of a properly defined framework. Procedure will be laid down for internal risk management also.

The board should implement policies and procedures which should include:

a) staff responsibilities in relation to fraud prevention and identification;

b) responsibility of fraud investigation once a fraud has been identified;

c) process of reporting on fraud related matters to management;

d) reporting and recording processes to be followed to record allegations of fraud;

e) requirements of training to be conducted on fraud prevention and identification.

Source: Department of Public Enterprises (DPE) (2010), *Guidelines on Corporate Governance for Central Public Sector Enterprises*, New Delhi, India. *dpe.nic.in/sites/upload_files/dpe/files/gcgcpse10.pdf*.

Responsibilities at the board level

Consistent with the OECD Principles and SOE Guidelines, almost all respondents identify risk management principally as a responsibility for SOE boards of directors. The national approaches fall in three categories namely i) mandate or encourage the establishment of risk committees; ii) entrust risk management to the board audit committees; or iii) stipulate an overall responsibility for the board to manage risk (according to national law, essentially an application of the duty of care). Practices vary not only across countries, but also by enterprise category, with the largest SOEs most likely to have specialised board committees. No respondent country mandates risk management committees for all SOEs.

The SOE Guidelines recommend that "when necessary" SOE boards should "set up specialised committees to support the full board in performing its functions, particularly with respect to [...] risk management" (Guideline VI.E). This clearly does not imply that every SOE should have a risk management committee, but that while the board as a whole would remain responsible for oversight of the risk management system, it could seek, where appropriate, the support of a committee dedicated to risk management issues.

The countries where a non-trivial number of SOE boards have established risk management committees include **Chile**, where government guidelines strongly recommend the establishment of a board-level committee responsible for risk management. Other countries where some of the larger SOEs have a risk management committee include **Germany**, **Israel** and **Korea**. In the **Netherlands**, **New Zealand**, **Norway** and **Switzerland** the large SOEs mostly have established board audit committees which are mandated to deal with risk management.

Among the countries that rely on the whole board of directors to manage risk (also including, among others, **Finland** and **Japan**), **India** provides an interesting example. The ownership co-ordination function (Department of Public Enterprises – DPE) has issued mandatory governance guidelines to SOEs which, among other things, stipulate how the

Table 1.2. **Risk governance requirements/recommendations for non-listed SOEs**

	Risk governance standards for non-listed SOEs	Legal/regulatory approach		
		Apply the same standards as for listed companies	Risk governance standards for listed companies (Table 1)	Implement special standards for non-listed SOEs
Argentina	Yes	–	L/R/C	●
Australia				
Austria	No	–	L/C	–
Belgium				
Brazil				
Canada				
Chile	Yes	–	R	●
Czech Republic	No	–	–	–
Denmark				
Estonia				
Finland	Yes	●	C	–
France				
Germany	No	–	L/C	–
Greece				
Hong Kong, China	No	–	R/C	–
Hungary				
Iceland				
India	Yes	–	L/C	●
Indonesia				
Ireland				
Israel	Yes	–	L/R	●
Italy	Yes	●	L/C	–
Japan	Yes	–	L	●
Korea	No	–	–	–
Lithuania	Yes	–	C	●
Luxembourg				
Mexico	Yes	–	L	–
Netherlands	Yes	●	C	–
New Zealand	No	–	–	–
Norway	Yes	–	L/C	●
Poland	No	–	L	–
Portugal	Yes	–	–	●
Saudi Arabia				
Singapore	Yes	–	C	–
Slovak Republic				
Slovenia	Yes	–	L	–
Spain	No	–	L/C	–
Sweden	Yes	●	C	–
Switzerland	Yes	–	L/C	●
Turkey	No	–	L/R	–
United Kingdom	Yes	–	C	–
United States	No	–	L/R	–

Notes: "**L/R/C**" denote laws, regulations, and codes or principles respectively. "**–**" denotes the absence of a specific requirement or recommendation.
Source: Country responses to OECD peer review questionnaire.

boards must be informed of the companies' risk taking (Box 1.6). It appears that Indian regulators may be particularly concerned with the risks emanating from irregular corporate practices.

Finally, another matter of some concern arises from the fact that in most jurisdictions the questionnaire responses make no mention of mechanisms to ensure that the risk management system is tailored to the risks faced by SOEs. Apart from general requirements, governments do not usually define a specific risk management system, so that each SOE is required to define it on its own responsibility. Moreover, in countries with federal systems, the federal government may not have information on risk-taking by SOEs owned by sub-national levels of government.[15]

Owner's risk

The question whether, at the level of the ownership function, there were any specific mechanisms in place to monitor the risk exposure in portfolio companies and assess the ultimate contingent liabilities for the state, was addressed only by a few respondents. Apparently, most ownership functions consider that their on-going monitoring of their SOE portfolio and benchmarking against performance criteria provides security enough. Another factor may be that, since an increasing proportion of SOEs are limited liability companies where the state does not carry formal liabilities beyond its paid-up capital, there is little appetite for dealing with the risk of contingent liabilities arising from SOE ownership. Considering the large liabilities that a number of OECD governments have assumed through this channel in recent years (especially through financial institutions that were either state-owned at the outset or considered "too big to fail"), this might be an area that merits further consideration.

One exception from this general observation is provided by **Korea**. An extensive public reporting system disclosing the current status of the balance sheet of the consolidated SOE sector is in operation. Furthermore, as previously discussed by the Working Party, owing to the fluidity of the situation of a large number of public institutions in **Korea** (who may or may not qualify as SOEs according to the size of their commercial earnings – which either places them inside or outside the general government), the liability situation is monitored closely.

Switzerland also considers its SOEs as part of the government's overall risk management system. In the Swiss case the onus is less on the balance sheets and more on the risk of fiscal fluctuations and the non-fulfilment of public tasks. Finally, the laws of **New Zealand** mandate the government to specify fiscal risks emanating from enterprise ownership in its annual fiscal budgets. The categories of risks include significant potential decisions or events which are "reasonably possible" and may materially affect fiscal revenues, expenses or the public balance sheet.

Notes

1. The internal control guide provided a major conceptual development by describing internal control as part of a process, rather than bolted on activities, which had five main components: i) a control environment; ii) risk identification; iii) control activities; iv) information and communication; and v) monitoring. Each part of this model was designed to support three key corporate objectives: the continuity of the business; timely and accurate financial reporting; and compliance with local laws and regulations. A final third dimension of the model was control activities that were expected to be carried out throughout the organisation.
2. The ERM guide developed three additional components: objective setting, event identification; and risk response. The ERM framework comprises: i) internal environment; ii) objective setting; iii) event identification; iv) risk assessment; v) risk response; vi) control activities; vii) information and communication; and viii) monitoring.

3. In the view of Anderson (2009), neither COSO nor Turnbull provides a helpful approach to the mechanics of creating an effective and lasting risk management and assurance framework over the long term. Missing elements include: risks are frequently not linked to strategy; risk definitions are often poorly expressed and have been reduced to the smallest number of words possible; the need for someone or something to make sure that the whole process takes place is not developed; not all involved stakeholders are considered and; only lip service is paid to important parts of the company's value chain that are outsourced, or where there is a dependence on key suppliers or joint venture partners.
4. In Germany, the risk management rules, being part of the company law, apply to all stock companies, both listed and unlisted.
5. More specific guidance and standards are also provided in Austria (Corporate Governance Code and ONR Standard 49000), and in South Africa (King 3 report).
6. Whereas many countries require companies to promptly report on a major deterioration in their financial situation, notably in cases where their continuation on a going-concern basis is under threat, this (*ex post*) crisis management is not the same as (*ex ante*) risk management.
7. Chief risk officers are usually required only for financial institutions.
8. No such standards exist, however, in NASDAQ's listing rules, and some have expressed concerns that audit committees may not be the right body to be charged with risk oversight. See e.g. Choi (2013) and NYC Bar (*www2.nycbar.org/pdf/report/uploads/20072409-NYSEListedCompanyRules.pdf*).
9. The same does not apply to NASDAQ.
10. In a number of OECD countries the central government is to some degree prevented – e.g. constitutionally or via administrative law – from interfering in the business activities of lower levels governments. In some countries, financial institutions are not technically considered as SOEs.
11. In Finland, for example, it is clearly stated in the government policy that the corporate governance code is to be applied as a model for the governance of and reporting by unlisted SOEs.
12. In India, for example, a specific guideline for the corporate governance of SOEs requires the establishment and periodical review of the procedure for informing the board about risk assessment and minimisation procedures.
13. An exception is made for the particularly commercially oriented "navratnas" and "maharatnas" that operate at higher levels of autonomy.
14. In the case of New Zealand, the fact that SOE debt is not subject to government guarantees must be explicitly stated when the liability is incurred.
15. Again, this situation has been cited in the press as a factor believed to have contributed to a host of large losses at certain publicly owned enterprises in recent years.

Bibliography

Anderson, R. (n.d.), *Risk Management & Corporate Governance, www.oecd.org/corporate/corporateaffairs/corporategovernanceprinciples/42670210.pdf*.

Anderson, R. (2011), *Risk Appetite & Tolerance*, Institute of Risk Management, London, *www.theirm.org/publications/documents/IRMRiskAppetiteFullweb.pdf*.

Basel Committee on Banking Supervision (2010), *Principles for Enhancing Corporate Governance*, *www.bis.org/publ/bcbs176.pdf*.

Beasley, M., B. Branson and B. Hancock (2012), *Current State of Enterprise Risk Oversight*, *http://poole.ncsu.edu/vol2/erm/ee/i/weblogs/research-documents/AICPA_ERM_Research_Study_2012_Final_Submission_July_16,_2012.pdf*.

Beasley, M. (2013), a.o., *Executive Perspectives on Top Risks 2013*, *www.protiviti.com/en-US/Documents/Surveys/NC-State-Protiviti-Survey-Top-Risks-2013.pdf*.

Choi, I. (2013), *When Do Companies Need a Board-Level Risk Management Committee?*, *www.gcgf.org/wps/wcm/connect/444c0e804ef2b9df9e1bdf3eac88a2f8/PSO+31.pdf?MOD=AJPERES*.

Committee of Sponsoring Organisations of the Treadway Commission (COSO) (2004), *Integrated Framework*, *www.coso.org/documents/COSO_ERM_ExecutiveSummary.pdf*.

Committee of Sponsoring Organisations of the Treadway Commission (COSO) (2012a), *Risk Assessment in Practice*, *www.coso.org/documents/COSOAnncsOnlineSurvy2GainInpt4Updt2IntrnlCntrlIntgratd Frmwrk%20-%20for%20merge_files/COSO-ERM%20Risk%20Assessment%20inPractice%20Thought%20Paper%20OCtober%202012.pdf*.

Committee of Sponsoring Organisations of the Treadway Commission (COSO) (2012b), *Understanding and Communicating Risk Appetite*, *www.coso.org/documents/ERM-Understanding%20%20Communicating %20Risk%20Appetite-WEB_FINAL_r9.pdf*.

Department of Public Enterprises (DPE) (2010), *Guidelines on Corporate Governance for Central Public Sector Enterprises,* New Delhi, India, *http://dpe.nic.in/sites/upload_files/dpe/files/gcgcpse10.pdf*.

Directors and Chief Risk Officers Group (DCRO) (2013), *Qualified Risk Director Guidelines*, *www.the governancefund.com/DCRO/PDF/Qualified_Risk_Director_Guidelines.pdf*.

Financial Reporting Council (2011), *Boards and Risk*, *www.frc.org.uk/FRC-Documents/FRC/Boards-and-Risk-A-Summary-of-Discussions-with-Comp.aspx*.

Financial Reporting Council (2013), *Risk Management, Internal Control and the Going Concern Basis of Accounting* (consultation Paper), *http://frc.co.uk/Our-Work/Publications/FRC-Board/Consultation-Paper-Risk-Management,-Internal-Contr-File.pdf*.

Financial Stability Board (FSB) (2013), *Thematic Review on Risk Governance*, *www.financialstability board.org/publications/r_130212.pdf*.

Financial Stability Board (FSB) (2013), *Principles for an Effective Risk Appetite Framework*, *www.financial stabilityboard.org/publications/r_131118.pdf*.

Frigo, M.L. (2009), *Strategic Risk Management: The New Core Competency.*

Group of Thirty (2012), *Toward Effective Governance of Financial Institutions*, *www.group30.org/images/PDF/ TowardEffGov.pdf*.

Hau, H. and M. Thum (2009), *Subprime Crisis and Board (In-)Competence: Private vs. public banks in Germany*, *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1360698*.

Institute of Directors in Southern Africa (2012), *King Code of Governance for South Africa* ("King 3 report"), *www.iodsa.co.za/resource/collection/94445006-4F18-4335-B7FB-7F5A8B23FB3F/King_Code_of _Governance_for_SA_2009_Updated_June_2012.pdf*.

International Corporate Governance Network (ICGN) (2010), *ICGN Corporate Risk Oversight Guidelines*, *https://www.icgn.org/files/icgn_main/pdfs/best_practice/icgn_cro_guidelines_(short).pdf*.

International Finance Corporation (IFC) (2012), *Risk Taking: A Corporate Governance Perspective*, *www1.ifc.org/wps/wcm/connect/9ff11a804c40464698dddaf12db12449/RiskGovJuly2012.pdf?MOD=AJPERES*.

Institute of International Finance (IIF) (2012), *Governance for Strengthened Risk Management*, *www.iif.com/download.php?id=PTVGcYdhz8I*.

Institute of Risk Management (2010), *A Structured Approach to Enterprise Risk Management*, *www.theirm.org/documents/SARM_FINAL.pdf*.

Institute of Risk Management (2012), *Risk Culture*, *www.theirm.org/documents/Risk_Culture_A5 _WEB15_Oct_2012.pdf*.

Manifest information Services (2010), "Board Practices: Incentives and Managing Risks – United Kingdom, Sweden, Portugal, Brazil and Japan", Report commissioned by the OECD (unpublished).

McKinsey&Company (2011), *Governance since the Economic Crisis*, *www.mckinseyquarterly.com/ Governance_since_the_economic_crisis_McKinsey_Global_Survey_results_2814*.

McNulty, T., C. Florackis and P. Ormrod (2013), "Boards of Directors and Financial Risk during the Credit Crisis", *Corporate Governance: An International Review*, *http://onlinelibrary.wiley.com/doi/10.1111/ corg.12007/pdf*.

National Association of Corporate Directors (2009), *Risk Governance: Balancing Risk and Reward www.oliverwyman.com/media/riskbrc-execsummary%282%29.pdf*.

New York Stock Exchange (n.d.), *Listed Company Manual* (Section 303A.07) *http://nysemanual. nyse.com/LCMTools/PlatformViewer.asp?selectednode=chp_1_4_3_11&manual=%2Flcm%2Fsections%2Flc m-sections%2F*.

OECD (2011), "Board Practices: Incentives and Governing Risks", *Corporate Governance*, OECD Publishing, *http://dx.doi.org/10.1787/9789264113534-en*.

OECD (2010), *Corporate Governance and the Financial Crisis – Conclusions and emerging good practices to enhance implementation of the principles*, OECD, Paris, *www.oecd.org/daf/ca/corporategovernance principles/44679170.pdf*.

OECD (2009), *Corporate Governance and the Financial Crisis: Key Findings and Main Messages*, OECD, Paris, *www.oecd.org/corporate/ca/corporategovernanceprinciples/43056196.pdf*.

Parsons, C.(2011), *Roads to Ruin*, *www.airmic.com/roads-ruin-study-major-risk-events-their-origins-impacts-and-implications*.

Pergler, M. (2012), *Enterprise Risk Management: What's different in the corporate world and why*, *www.mckinsey.com/~/media/mckinsey/dotcom/client_service/risk/working%20papers/40_whats%20different%20in%20the%20corporate%20world.ashx*.

Renn, O. (2008), *Risk Governance: Coping with Uncertainty in a Complex World*, *www.ortwin-renn.de/node/7*.

Taleb, N.N. (2004), *Fooled by Randomness*, *www.fooledbyrandomness.com*.

Chapter 2

Norway: The corporate governance framework and practices relating to risk management

This chapter, part of the sixth peer review based on the OECD Principles of Corporate Governance, *summarises the corporate governance framework and practices relating to corporate risk management in Norway, with a focus on the framework for and practices of state-owned enterprises. The chapter was prepared by the OECD Secretariat (Daniel Blume and Winfrid Blaschke).*

2.1. Introduction

Norway's equity market provides a number of distinctive features which make Norway an interesting case for an in-depth review of risk management policies and practices. Its market is characterised by a large proportion of public ownership (36.3% of overall market capitalisation, covering both state and municipal-level ownership), both directly and through *Folketrygdfondet*, the state-owned asset manager responsible for managing the Government Pension Fund Norway. Foreign shareholders comprise a similar proportion of market capitalisation in the Norwegian equity market (35.8%). Shareholding by private companies and private investors make up a much smaller proportion of share ownership (18%), with mutual funds far behind comprising just 7% of market capitalisation. The importance of state ownership is reflected in the fact that a single, majority state-owned company, Statoil, accounts for 31.85% of domestic firm market capitalisation, and the five largest domestic listed companies, all with at least one-third state-ownership, account for 62%.[1]

In this context, the state plays an active and engaged leadership role, as a minority shareholder through Folketrygdfondet, as a majority or significant shareholder in eight large listed companies, majority owner of another 25 non-listed enterprises and as the full owner of 17 statutory corporations (OECD, 2013).

Whether the state's role and long-term interest in the Norwegian market contributes to a higher or lower risk appetite was a subject of some discussion during the OECD review and will be addressed in greater detail later in this report. In addition, it is possible that the state gives greater attention to some elements related to risk in its oversight of companies – notably on environmental and social issues and executive remuneration – than some other shareholders. While the general position of the state is that risk management is essentially the responsibility of the board, the state also undertakes risk assessment on a regular basis as part of its ownership administration. Strong attention to risk management has also arisen when issues have emerged in the press related to reputational risk (such as corruption cases, compliance failures, treatment of the environment, human and labour rights). Such cases generally prompt follow-up by the state as shareholder through regularly held meetings with management to ensure that the risks are being properly managed and addressed.

To be sure, the state's role as shareholder should not be over-emphasized, as Norway's overall corporate governance legal and regulatory framework and Code of Practice for Corporate Governance apply to a wider universe of 360 Norwegian public limited liability companies, subjecting them to disclosure and other requirements relevant to risk management discussed in this report. Nevertheless, the state's active role as a long-term shareholder and its general priorities and approach have an important influence, offering some distinctive issues for consideration for this report.

Overall, within the public limited liability legal form, approximately 255 companies are listed on the Oslo Stock Exchange (*Oslo Bors*), including 34 on the "Oslo Axess" segment for small and medium-sized enterprises. By contrast, one research report found

94 000 private limited liability companies in Norway.[2] Market capitalisation accounted for 50.6% of GDP as of 2012, compared to an OECD member average of 86.5%. Liquidity is also relatively low, with the value of shares traded accounting for 56% of market capitalisation in 2012, well below the OECD average of 102%, according to World Bank indicators.[3]

2.2. Risk management standards and codes

Norway's Public Limited Liability Companies Act does not specifically set out requirements for risk management, but board responsibilities are considered to include risk management through the more general requirements of Sections 6-12 and 6-13, which set out board duties with respect to managing and supervising the company. This includes a requirement that the board of directors "shall ensure a proper organisation of the business of the company", and that it "shall keep itself informed of the company's financial position and are obliged to ensure that its activities, accounts and capital management are subject to adequate control". Section 6-43 of the Act further specifies requirements for the audit committee, including its responsibilities for internal control, risk management and internal audit. Relevant legal requirements for financial sector firms[4] are elaborated in much greater detail through regulation 2008-09-22 No. 1080 on risk management and internal control, issued in 2008 by the Ministry of Finance (the specific requirements for boards of directors, the CEO and the company as a whole are described in later sections of this report).

In addition, the Accounting Act was amended in 2011 to require all listed companies to produce an annual corporate governance report, which according to Section 3-3b second paragraph requires, among other elements, that the report include "a description of the main elements of the company's (and where applicable the group's) systems for internal control and risk management in relation to the financial reporting process". The Financial Supervisory Authority of Norway (*Finanstilsynet*) reviews the financial reporting and annual reports, including the corporate governance reports, of at least 60 listed companies annually to ensure that the reports contain the required information (but does not control for the quality of this information).

The Norwegian Code of Practice for Corporate Governance is seen as providing the main guidance to public limited liability companies to interpret these broader legal requirements. The Code of Practice addresses 15 major topics, including Chapter 10 specifically covering risk management and internal control. Companies are legally required to provide information on whether they comply with the recommendations and to explain when they do not. The Code's first chapter, based on stock exchange listing requirements, calls for each company to provide a more comprehensive explanation, including information on its compliance with each of the recommendations, as well as to justify any deviations from the Code and to explain what alternative solutions it has selected.

The chapter on risk management and internal control is introduced by the following general recommendation:

> "*The board of directors must ensure that the company has sound internal control and systems for risk management that are appropriate in relation to the extent and nature of the company's activities. Internal control and the systems should also encompass the company's corporate values, ethical guidelines and guidelines for corporate social responsibility. The board of directors should carry out an annual review of the company's most important areas of exposure to risk and its internal control arrangements.*"

The Code also includes a much more detailed "Commentary" which states that "the objective for risk management and internal control is to manage, rather than eliminate, exposure to risks related to the successful conduct of the company's business and to support the quality of its financial reporting".

The commentary provides more specific descriptions of what should constitute effective internal control, the recommended components of an annual review of risk areas and the internal control system, and the main features to be included in the board of directors' reporting of the company's internal control and risk management systems (full text provided below under section on risk management guidance).

The Norwegian Code was developed by the Norwegian Corporate Governance Board (NCGB), which includes the participation of the Norwegian Shareholders Association, Norwegian Institute of Public Accountants, the Institutional Investor Forum, Finance Norway, the Norwegian Society of Financial Analysts, the Confederation of Norwegian Enterprise, the Oslo Stock Exchange, Association of Private Pension Funds and Norwegian Mutual Fund Association. They have issued seven versions of the Code since it was first published in 2004, with the risk management and internal control chapter introduced in 2006, taking effect in 2007. The 2006 version of the Code indicates that a main reason for the addition was European Union Directive 2006/46/EF, which included a requirement that the board of directors of a listed company issue a statement on corporate governance in its annual report, and that as part of this statement, the board must report on the main features of the company's internal control and risk management systems with respect to the financial reporting process. While Norway is not a member of the EU, it is part of the European Economic Area (EEA) agreement which obligates it to implement most of the internal market regulation of the EU.

One issue on which the Code's recommendations differ from most corporate governance Codes in the European Union is on the role of internal audit. Norway's Code is one of the few in the EEC area that does not specifically recommend that companies maintain an internal audit function (ECIAA, 2012),[5] and in Norway, only an estimated 10% of listed companies have internal auditors, according to the Norwegian Institute of Internal Auditors.

Market participants suggested that in general, company compliance with the recommendations of the Norwegian Code of Practice for Corporate Governance (including the chapter on risk management) is high. EY (formerly Ernst & Young) conducts annual reviews of compliance with the Code and has found a general improvement in compliance over time. However, their survey only covers up to 70 of the largest listed companies on the main exchange, and it was suggested that compliance is probably not as high among smaller listed companies.

In addition to guidance provided by the Norwegian Code of Practice, Norwegian companies that cross-list in other markets such as in the US or the UK face additional requirements related to risk management, internal controls and disclosure, for example, with respect to the requirements for internal control established under Sarbanes Oxley and 20-F risk disclosure requirements.

Corporate governance framework

Norway's corporate governance framework, while fitting within the overall requirements of relevant EU directives, has a number of distinctive characteristics which may be seen as consistent with a Nordic model of governance. Norwegian companies

generally have a single-tier board, and the CEO cannot be a member of it. Furthermore, the Corporate Governance Code recommends that neither the chief executive nor any other executives of the company should serve on the board.

Companies with more than 200 employees may also have a corporate assembly, which plays a supervisory role that includes authority to take decisions on major issues such as large-scale investments or restructuring. The corporate assembly consists of at least 12 members, one-third of whom are elected by employees, and two-thirds by shareholders. However, most companies and their employees have chosen to opt out of having a corporate assembly, in which case a system of co-determination applies under which employees can elect one more than one-third of the board (Fulton, 2013). Thus, the corporate assembly system does not appear to play a major role, but one of the principles behind it, to ensure employee representation, is well integrated into Norwegian boards in general. Smaller public limited liability companies also may follow this system of co-determination if employees formally request it, but the requirements for employee representation are smaller (up to one-third for companies with more than 50 employees; at least one employee board member for companies with more than 30 employees).

Norway is also known for its pioneering requirement, established in 2006 and implemented in 2008, requiring that each gender have at least 40% presence on the boards of public limited liability companies (applying also to employee representation). This requirement was first established for state-owned companies beginning in 2004. It has had a major impact on board composition; since 2006, the percentage of women on public limited liability company boards has risen from 18% to 40% in 2009. In private limited liability companies where no such requirement exists, the proportion of female board members has remained stable during the same period at between 16% and 17%. Women selected to the board were also reported to have different demographic characteristics than their male counterparts (younger, more education, less ownership interests in the companies whose boards they serve on) (Teigen and Heidenreich, 2010).

During the same period, the number of public limited liability companies decreased from 505 to 382. However, this reflected the continuation of a declining trend in public limited liability companies that had already begun in 2001, when 630 were registered in Norway. It should also be noted that the number of listed public limited liability companies has declined at a much slower rate than the more widely used public limited liability legal form, from 195 in 2006 to 184 in 2012, according to World Bank figures.[6] Only a third of the respondents in a survey of companies that had switched to the private liability form cited the quota regulation as a factor in their decision, and only 7% cited it as the *only* reason. The leading reason given by 60% of the respondents was that it was "more convenient/ practical to be a private limited company" (Teigen and Heidenreich, 2010). This broader concern about the costs of following Public Limited Liability Company regulation is relevant for any consideration that may be given to establishing additional requirements in Norway with respect to risk management.

Some company representatives and market observers interviewed for this report suggested that the recent change in board composition may have had an impact on board behaviour, including in its consideration of risk. However, such assertions were difficult to verify. Two reports focusing on the UK suggest that boards with better gender balance pay more attention to audit and risk oversight and control than all-male boards, and that they are more likely to pay attention to managing and controlling risk (Crowley, 2011; and

UK government, 2011). Other studies have sought to show the impacts of gender-balanced boards on corporate value and corporate performance, but an OECD review of this research found the results to be ambiguous, with both positive and negative correlations and other problems related to the difficulties of establishing causality (OECD, 2012).

Risk management guidance

The Norwegian Code's Chapter 10 on risk management and internal control provides the following more detailed guidance to supplement the previously cited general recommendation:

Internal control comprises guidelines, processes, duties, conduct and other matters that:

- *Facilitate targeted and effective operational arrangements for the company and also make it possible to manage commercial risk, operational risk, the risk of breaching legislation and regulations as well as all other forms of risk that may be material for achieving the company's commercial objectives.*
- *Contribute to ensuring the quality of internal and external reporting.*
- *Contribute to ensuring that the company operates in accordance with the relevant legislation, regulations and internal guidelines for its activities, including the company's corporate values, its ethical guidelines and its guidelines for corporate social responsibility.*

The board of directors must form its own opinion on the company's internal controls, based on the information presented to the board. Reporting by executive management to the board of directors should give a balanced presentation of all risks of material significance, and of how the internal control system handles these risks.

The company's internal control system must, at a minimum, address the organisation and execution of the company's financial reporting. Where a company has an internal audit function, it must establish a system whereby the board receives routine reports and ad hoc reports as required. If a company does not have such a separate internal audit function, the board must pay particular attention to evaluating how it will receive such information.

Ethical guidelines should provide guidance on how employees can communicate with the board to report matters related to illegal or unethical conduct by the company. Having clear guidelines for internal communication will reduce the risk that the company may find itself in situations that can damage its reputation or financial standing.

Annual review by the board of directors

The board's annual review of risk areas and the internal control system should cover all the matters included in reports to the board during the course of the year, together with any additional information that may be necessary to ensure that the board has taken into account all matters related to the company's internal control.

The review should pay attention to:

- *changes relative to previous years' reports in respect of the nature and extent of material risks and the company's ability to cope with changes in its business and external changes;*
- *the extent and quality of management's routine monitoring of risks and the internal control system and, where relevant, the work of the internal audit function;*
- *the extent and frequency of management's reporting to the board on the results of such monitoring, and whether this reporting makes it possible for the board to carry out an overall evaluation of the internal control situation in the company and how risks are being managed;*

- *instances of material shortcomings or weaknesses in internal control that come to light during the course of the year which have had, could have had or may have had a significant effect on the company's financial results or financial standing; and*
- *how well the company's external reporting process functions.*

Reporting by the board of directors

The board of directors must by law provide an account of the main features of the company's internal control and risk management systems as they relate to the company's financial reporting. This account should include sufficient and properly structured information to make it possible for shareholders to understand how the company's internal control system is organised. The account should address the main areas of internal control related to financial reporting. This includes the control environment, risk evaluation, control activities, information and communication and follow-up.

If the company uses an established framework for internal control this should be disclosed. Examples of this include the framework for risk management and internal control published by the Committee of Sponsoring Organisations of the Treadway Commission.[7]

EY's annual reviews of company compliance with the Code have found that the large majority of Norway's largest companies comply with the Code's recommendations on risk management and internal control, but that the quality of their reporting varies. For the 2012 reporting year, EY reviewed and rated the compliance of 51 listed companies on the main index on a scale of 1 to 6, with 1 indicating no provision of information and 6 indicating leading practice. Ten companies were given ratings of 5 or 6, considered to have at least some outstanding practices, while another 34 were given ratings of 3 or 4, indicating general compliance but with varying quality of information. Only five companies received ratings of 1 or 2, indicating no or only partial provision of information. EY reported that resource constraints preclude it from surveying all listed companies, but that among smaller companies, compliance was likely to be lower.

By contrast, in the first review of compliance with the recommendation for the 2007 reporting year, 25 of 74 companies provided no information and another 14 provided only partial information. Despite EY's development of stricter criteria for judging compliance and what is considered outstanding practice over time, the average company rating has risen from 2.9 in 2008 to 3.6 in 2013.

Nevertheless, it was also noted that the ratings of how companies report on risk do not guarantee that such companies have good risk management, and that some companies that have fared well in the EY survey have nevertheless had problems with unforeseen risks emerging.

2.3. The role of Norwegian boards of directors and board-level committees

Within the Norwegian corporate governance framework, board members have important responsibilities for the overall management of the company's affairs, including the strategy, organisation, financial structure of the company and oversight of risk management and internal controls, whereas the day-to-day management belongs to the authority of the general manager (Sjaafjell and Kjelland, 2010).

More specifically, Norway's financial sector regulation on risk management and internal controls requires that the board ensure "appropriate risk management systems

and internal controls". While these regulations do not apply to non-financial sector firms, they may be seen as also influencing non-financial firm practices. Its provisions call for:

1. a clear division of responsibilities between the board and management set out in the instructions for the board and CEO;
2. a clear organisational structure;
3. the establishment of goals and a strategy for the enterprise, as well as general guidelines for the business; it shall state the risk profile that the undertaking shall have, as well as the risk limits that apply where this is relevant;
4. the establishment of principles for risk management and internal control for the enterprise as a whole and within each business area;
5. ensuring that risk management and internal control are established in accordance with the laws, regulations, statutes and instructions from the FSA and guidelines issued by the board to management, including the processing of reports prepared in accordance with Section 8 and Chapter 4;
6. ensuring that risk management and internal control are implemented and monitored, including the processing of reports prepared in accordance with Section 8 and Chapter 4;
7. determining whether the company should have an internal audit in accordance with Section 9;
8. evaluating its performance with respect to risk management and internal control at least annually.[8]

Based on the EY survey results of compliance with the Code and on discussions with both the regulatory authorities as well as a sample of Norwegian companies, there appears to be high levels of compliance with both the regulatory requirements as well as with the Code's recommendations that boards of directors review major risks and internal control systems on at least an annual basis, and that the audit committee first considers the annual risk report in preparation for the board's annual review.

The Public Limited Liability Companies Act requires that all issuers of transferable securities listed on a regulated market have an audit committee. Among the audit committee's legally required functions are to "monitor the systems for internal control and risk management including the internal audit of the company to the extent such function is established" [Section 6-43(b) of the Act]. However, companies below a certain size threshold[9] may use the full board to function as an audit committee. The Code's recommendations with respect to the audit committee do not mention assessment of risk specifically, only recommending that the auditor present at least once a year to the audit committee a review of the company's internal control procedures, including identified weaknesses and proposals for improvement. There are no legal requirements or Code recommendations concerning the establishment of risk committees, and it is reportedly rare outside of the financial sector.

2.4. Risk management policies and structures in Norwegian companies

Norway's financial sector regulation on risk management, in addition to the responsibilities of the board enumerated above, also requires the CEO to:

1. Make sure to establish sound risk management and internal control based on an assessment of current risks in accordance with guidelines established by the board.

2. Continuously monitor changes in the entity's risks and ensure that the firm's risks are properly addressed in accordance with the board's guidelines.
3. Provide the board with relevant and timely information that is of importance to the company's risk management and internal controls, including information about new risks.
4. Ensure that the company's risk management and internal controls are documented.
5. Ensure that risk management and internal controls are implemented and monitored in a responsible manner.

The regulation additionally requires the CEO to prepare an annual assessment of risk for the board, that the company report a summary of its conclusions regarding the risk situation, and that its risk assessments also apply to parts of the business that are outsourced.

While it was not possible to obtain a complete overview of listed company risk management practices, interviews for this report with management representatives of six non-financial Norwegian companies – four listed and two fully state-owned – as well as representatives of different market and professional institutions, provided some indication of what is common practice among larger Norwegian companies.

These interviews indicated that practices within Norwegian companies are evolving. Norway (and possibly other Nordic countries) may tend to rely less on formal, hierarchical structures than some other European countries, and may make greater use of flat, informal structures. While all companies interviewed reported that they comply with the Norwegian Code and relevant regulations, the day-to-day issues that they grapple with on risk management tend not to be addressed by the Code or regulatory requirements. For example, the Code and regulations make no recommendation on the value of designating a chief risk officer with direct reporting lines to the board or audit committee. This type of structure in Norwegian companies appears to be rare. Generally the CEO or CFO has this responsibility, and lower-level risk officers report either to the CFO or CEO, or even in some cases to a manager who reports to the CFO. In some cases, they have authority to report directly to the audit committee or board chair if they have a concern that their management is not adequately addressing their concerns, but this was not reported as being necessary in practice. One company reported that it did not even have a lower-level person responsible for risk identification and reporting until 2010, and that until that point, the company followed a more decentralised model that did not necessarily link technical risks to business risks. This absence of high-level, centralised authority for risk comes from a perspective that risk is an important responsibility and factor to take into consideration across all lines of business, and that it is the line manager or line organisation that should "own" and address the risks in their line of business directly through risk treatment plans and implementation of risk treatment actions.

On the other hand, companies interviewed for this report have also established management co-ordination systems for assessing and reporting on risk across the company. A common approach to risk management within Norwegian companies is to have a management risk committee or corporate management board that brings together the different perspectives and expertise on risk in one body before it is considered by the audit committee or board. The chief financial officer may be responsible for financial risk and internal controls, the chief legal counsel for risks related to compliance, and a corporate social responsibility officer or human resources manager for issues related to health and safety, ethics, and environmental and labour standards. Frequently the CFO or CEO have a risk officer responsible for co-ordinating risk management information-

gathering processes that may feature both top-down guidance on important corporate-wide risks and strategic considerations as well as bottom-up gathering of information on the risks in different countries or different lines of business. These are presented to the management committee as "risk-mapping" or "heat" charts that identify the top 10 or 20 risks that the companies face. Using color-coded charts, the maps identify what are considered the most significant risks, based on a combination of probability and magnitude, that may receive the most attention in both management and board discussions. For each risk identified, companies establish mitigation plans or proposals for how the probabilities or magnitudes of such risks can be reduced.

Differences were reported, however, in terms of how these reports are used. Some companies reported that over time, the top 10 risks change very little and the board understands how they are being addressed, so the value of board discussions comes in terms of reviewing the development of risks over time, including what is new or has changed since the previous review, or in choosing an issue of priority to examine in greater depth.

It was also apparent from discussions that risk management systems and policies evolve significantly in response to actual experience with risk materialisation, particularly high-profile accidents or scandals that may be characterised as "Black Swan" events because they were unforeseen and caused major impacts (see Box 2.1 and the case of Statoil as an illustrative example).

Box 2.1. **Norway – Statoil's experience with risk management**

Among companies interviewed for this report, Statoil, Norway's largest company with a market value of approximately USD 74 billion at the end of 2012, has one of the most fully elaborated risk management systems. A number of key incidents have impacted on its risk management systems, two of which are highlighted below. Its officials note the wide array of risks specific both to working in the oil industry, and to its extensive operations in 35 countries, including some particularly high-risk environments. The importance of risk as a core part of its business led to the initiation of its Enterprise Risk Management (ERM) system in 1999, which included the establishment of a management "Corporate Risk Committee" headed by the CFO. The system has gradually evolved since then, including the first use of comprehensive risk mapping reporting processes in 2006. The corporate risk committee meets at least six times per year. The audit committee and the board receive reports on aggregated risk three times a year, but in addition to considering aggregate risks will choose to focus on one or two specific areas at each meeting.

Statoil undertook significant changes to its risk management following a bribery case involving illegal payments made to secure participation in the development of the Iranian South Pars gas development project, the so-called "Horton Affair", which came to light in 2004. Statoil settled the case with the US Department of Justice and Securities and Exchange Commission in 2006 under agreements that required it to pay a USD 10.5 million fine, a USD 10.5 million confiscation of benefits and a USD 3 million criminal penalty. In addition, Statoil agreed to work with an external compliance consultant for three years to evaluate its internal control systems and guidelines related to compliance with the US anti-corruption law. However, interviews suggested that the consequences of the case were of far greater magnitude, because of its impact on the company's reputation (which also can have a financial impact), the whole-scale changes at the level of CEO and the board in the immediate aftermath of the case, and a reduction in time available for management and the board to focus on strategy and other company business while being

Box 2.1. **Norway – Statoil's experience with risk management** *(cont.)*

occupied with its fallout. Statoil's 2009 Annual Report states that Statoil had taken several significant and concrete steps to prevent a similar case in the future, including anti-corruption training of Statoil personnel, with additional focus on groups among its employees deemed to be particularly exposed to corruption risk. Another practical step taken was the development of a risk-based procedure for vetting all new and significantly changed business relationships. Its web site contains a 64-page report setting out further details on its Anti-corruption compliance programme.

An important recent case was the January 2013 terrorist attack on the In Amenas gas facility in Algeria, which led to the deaths of 40 people, including five Statoil employees. In Amenas is operated as a joint venture between the Algerian national oil company Sonatrach, BP and Statoil. In the aftermath of this incident, the Statoil board of directors commissioned an investigation "to clarify the chain of events and to facilitate learning and further improvements within risk assessment, security and emergency preparedness". The investigatory team delivered its report to the board in September 2013, including 19 recommendations. Among the recommendations are calls for security training for all employees and managers with more targeted security training for managers and international assignees particularly in countries with higher security risks; open and clear communication of potential security risks to employees; and development of a security risk management system based on a standardised, open and well-defined security risk management methodology that will allow both experts and management to have a common understanding of risks, threats and scenarios, and evaluation of these. The report also calls for systematically developing and maintaining security risk management plans, and several steps to improve co-ordination and standardisation of emergency response planning.

The impact of ESG analysis

An additional common theme emerging from interviews with companies – different from other countries reviewed for this report – was the strong attention given to corporate social responsibility issues. This strong attention to risk comes from several directions; first, companies are legally required to report on their corporate social responsibility under the Norwegian Accounting Act Section 3-3c. In addition, companies interviewed for this report noted that there has been a growing interest among shareholders, including both the state and some institutional investors, to see how companies are dealing with these issues. But perhaps most importantly, the companies suggested that there is a strong business case for addressing these issues. All companies interviewed reported having designated someone in charge of dealing with corporate social responsibility issues, and these issues generally form an important part of the overall assessment of risks related to health and safety, review of reputational risks and compliance with international norms with respect to labour and the environment, with particular sensitivity to operations in countries and with suppliers or other third parties in those countries that may follow different standards. This has led, for example, to companies giving greater emphasis to training on company codes of ethics and expectations with respect to the prevention of corruption.

The government's ownership policy states that the state "will be an active driving force in the work relating to corporate social responsibility and use the state ownership to ensure that the companies fulfil their social responsibility". It states that it expects all Norwegian companies to fulfil their social responsibility, regardless of whether they are privately or publicly owned, but that those with state ownership "must be leaders" within

their respective fields. The report defines CSR as "what companies do on a voluntary basis over and above complying with existing laws and regulations in the country in which they operate", and that "Companies integrate social and environmental considerations in their daily operations and in relation to their stakeholders". While historically CSR may have been seen as the involvement of companies more broadly in their communities through provision of services and support for humanitarian and cultural activities, the current CSR focus is on the company's own operations and supply chain, and the impacts of its core business on society.

In practice, this means that the ministries as owners hold annual meetings with management on how the company is dealing with CSR issues, including how CSR is integrated in the companies' business planning. In addition, they hold quarterly management meetings which may also touch on social responsibility issues, especially when there are difficult issues to be handled. Issues attracting media coverage and stakeholder concern, i.e. risks to reputation, appear to attract the particular attention of the government. For example, two state-owned companies, Telenor and Yara International, were the subject of particular attention in 2012 due to allegations of corruption. In the case of Telenor, the company faced considerable losses in its India operations after its India-based partner, Unitech Wireless, became the target of corruption charges, raising questions about whether Telenor had accurately assessed the risks of partnering with the company, in which it had taken 67% ownership. Telenor dissolved its partnership with Unitech by the end of 2012. Yara International, a chemical and fertiliser company, is under investigation by the Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime for making unacceptable payments.

However, it was also noted that the government as shareholder conducts its own ESG analyses and raises issues on a proactive basis. The Government Pension Fund Norway 2012 Ownership Report provides a number of concrete examples of its interventions, generally on a proactive basis, engaging in dialogue with companies in relation to development of anti-corruption guidelines and procedures, reporting on greenhouse gas emissions and other environmental issues, as well as the development of guidelines on human rights and employee rights in the supply chain.

2.5. External assessments of the risk management framework

The state as owner

The state's role as direct owner of commercially-oriented companies is primarily exercised through the Ministry of Trade and Industry's Ownership Department, which has responsibility for 21 enterprises with 100%, controlling or significant minority ownership. The Ministry of Petroleum and Energy administers the shareholdings for Statoil and five other SOEs, while Ministry of Transport has the largest portfolio of commercially-oriented SOEs among other ministries. However, these holdings account for just 16% of the state's asset management as of 30 June 2010. Folketrygdfondet's Government Pension Fund Norway has another 5%, which are invested in approximately 50 Norwegian companies limited to no more than 15% of any company, and approximately 100 Nordic companies outside of Norway at levels not exceeding 5% per company (Norwegian Ministry of Trade and Industry, 2011). The state also has indirect investments in equities abroad, limited to 10% of any individual company. These investments are made by Norges Bank, the Central Bank of Norway wholly

owned by the state through its management of the Government Pension Fund Global, Norway's sovereign wealth fund (funded through state-owned petroleum profits).

For state-owned companies with commercial objectives or mainly commercial objectives (including partially state-owned listed companies), the state maintains a general, overall objective of commercial profitability, a high level of value creation and the highest possible return on investment over time. This is pursued by organising these state-owned companies as independent legal entities under which the state essentially eschews influence of their day-to-day business, instead exercising its ownership interests through decisions of the annual general meeting and involvement in nomination and election of board members. Within this framework, the recurrent theme among representatives of the government and the pension fund is that oversight of risk management and internal controls is the responsibility of the board, and that it is not the state's role to intervene in these processes as a shareholder. For this reason, the state gives particular priority to establishing effective nomination processes that ensure the necessary competencies and experience on the board to manage risk and other board responsibilities. Ministry of Trade and Industry authorities reported that the process of identifying candidates for the board became more systematic with the advent of the requirement (established in 2002 for fully state-owned companies and in 2006 for listed companies) that the board comprise at least 40% of each gender. Boards conduct evaluations that are used by nomination committees, together with the committees' own analysis (after interviewing all members of the boards and making its own assessment of the companies' main business challenges and future risks), to help develop profiles of what competencies and experience are needed. The Ministry of Trade and Industry also makes use of head-hunting firms to help identify candidates for consideration.

Although this nomination process is not directly on the subject of risk management *per se*, it is important for understanding the mind-set of the government in terms of how the ownership function prioritises the use of its resources and the extent to which it trusts the board to effectively handle risk management issues directly.

Nevertheless, the state as direct owner as well as through its pension fund holdings has an important influence on how companies approach risk issues. Its role and interests are exercised not only through the board nomination process and participation in annual shareholder meetings, but also through quarterly meetings with management, which cover a range of issues, such as the appraisal of financial trends, briefings concerning strategic issues involving the companies, and problem areas relating to social responsibility.[10] In addition, the state's expectations regarding return on investment and dividends is generally communicated directly to the chairman of the board. The board retains the authority to decide on the dividend, while in the case of a fully-state-owned company, the state may determine the dividend through the AGM.

The state also exerts an oversight role with respect to risk as any other major shareholder in the case of major transactions. The listed and partly state-owned aluminium producer Norsk Hydro's USD 5.3 billion purchase of Brazilian-based Vale, completed in 2011, is one example in which the decision required extensive discussions and review by the state prior to the final decision. The state participated in the amount of NOK 4.4 billion in a share capital expansion carried out in connection with the transaction, and an extensive risk assessment of the transaction was one element in the decision of the state to participate in the share capital expansion (which also had to be approved by the

Parliament). As a consequence of the transaction, the state's shareholding was reduced from 43.8% to 34.3%. The Ministry of Trade and Industry's shareholding unit has continued to monitor the risks associated with the implementation of this decision, including through recent participation in a Norsk Hydro management fact-finding trip to Brazil to interview Vale and Norsk Hydro Brazil-based management.

One question raised in the course of the review was how the state's ownership impacts on SOEs' risk appetite and risk-taking behaviour. In theory, state ownership could make a company more willing to take risks, for example, if it were perceived that the state offers "deep pockets" to bail a company out of trouble; or more risk averse, for example, if a company needed explicit approval of the state for actions associated with higher risks. The state may also implicitly influence risk-taking behaviour through the targets it sets for return on investment and dividends in the companies that it owns: if the targets are set too high, companies may have an incentive to take greater risks, whereas if they are too low, they may become more risk-averse. In practice, SOE managers interviewed in the course of this review suggested that they behave similarly to other companies, with an aim to maximise profits similar to private companies, within the constraints set out for them as state-owned companies. These constraints may include, for example, certain limits with respect to maintaining SOE head offices and associated functions such as research, innovation and technological development in Norway. A shareholder with at least one-third of a company's shares can provide blocking control over decisions requiring a two-thirds majority, such as the relocation of headquarters, the raising of share capital and amendments to the articles of association.

In addition, the state's policy on executive remuneration may be seen as reducing management incentive to take risks for short-term gain. The policy includes limits on the total variable salary component in any one year to no greater than six months' fixed salary, and a statement that share options and other similar schemes must not be used by companies in which the state has a shareholding. Share-based remuneration is permissible, but must be held for a fixed binding period of at least three years and "must be formulated so that it encourages a long-term contribution to the company".

The Government Pension Fund Norway's guidelines for executive remuneration also stress the importance of incentive schemes being designed to motivate "long-term value creation", but are somewhat more flexible regarding variable pay. Their guidelines allow for the use of option schemes while stressing the importance of calculating their real value, and suggesting that "a significant portion of the equities should be held for a minimum of three years". Representatives of the Pension Fund's management noted that the fact that its equity holdings are no greater than 15% for any company has an influence on its differing position.

Disclosure practices

As noted previously, Norwegian companies are required to report annually on their risk management and adequacy of internal controls. EY's review found high variability in the quality of such reporting, ranging from very general to some quite specific and detailed reports, with financial industry companies tending to devote more attention to their risk reporting. More extensive reporting is also undertaken by companies with respect to Sarbanes Oxley 20-F disclosure requirements, which may feature a detailed list of all credible eventualities without being too specific about how likely or prioritized the risks are. Legal officials interviewed for the report noted that this type of reporting is driven by

the necessity to guard against lawsuits that may fault a company for misrepresentation or failure to identify particular risks.

By comparison, companies' aggregate reporting on company risk to the board tends to be more nuanced, prioritising risk, highlighting probabilities and specific actions that may be taken to mitigate the risks. However, the confidential nature of these discussions and reports is essential to enable the board and management to be able to have a frank and full discussion of the company's risks and how to treat them.

External auditors

The external auditor plays an important role in the Norwegian risk management framework in terms of reviewing financial reports and the adequacy of internal controls, but is less relevant in terms of non-financial risks pertaining to compliance, health and safety, or CSR issues. The auditor is legally entitled to participate in the general meeting and must do so if the auditor's presence is considered necessary in relation to any of the items to be considered. The Norwegian Code goes a step further, stating an expectation that the board of directors make arrangements for the auditor to participate in all general meetings. The Code also recommends that the auditor present his or her findings to the audit committee at least once a year. A legal requirement of the Norwegian Audit Act stipulates that, except for small companies, the board must hold a meeting with the auditor at least once a year at which neither the CEO nor any other member of the executive management is present.

In the case of state-owned companies, the Office of the Auditor General may also undertake audits, but its impact on risk management issues in commercially-oriented SOEs appears to be limited. For wholly-owned companies, the OAG's reviews include an assessment of how risk is described in the minutes of board meetings, and what decisions the board makes regarding risk. In partly-owned companies, the OAG reported that it has limited access to information, and no access to minutes from board meetings. Hence, in partly-owned SOEs, risk management is only considered if there is publicly available information on the subject. If the risk assessment indicates that a wholly-owned company should be further investigated, this will normally be done through a performance audit or smaller review known as a comprehensive control. The OAG reported that in its reviews of commercially-oriented SOEs, it has only briefly and indirectly touched upon risk management issues.

The role of shareholders

The role of the state as a shareholder in risk management issues has been described at length, but less information was available on how active other shareholders (and stakeholders) are with respect to these issues. Companies interviewed for this report said that it depends on the shareholder – some never raise questions about risk management issues, whereas others, particularly those with a long-term orientation such as pension funds or other institutional investors that have signed on to the Global Reporting Initiative, may take a particular interest in how the company prepares for and reports on environmental, social and governance risks.

2.6. Conclusions

Risk management practices in Norway are evolving and appear to have been gradually improving since the Norwegian Code of Practice for Corporate Governance first introduced

its risk management and internal control recommendations in 2006. With the influence of the state as a major shareholder in Norwegian listed companies both through direct ownership and through Folketrygdfondet's Government Pension Fund Norway shares, companies' risk assessments appear to be broadly encompassing, focusing not only on financial risks and internal controls, but also on reputational and compliance risks, as well as risks related to corporate social responsibility issues.

Despite several revisions of the Norwegian Code since 2006, its recommendations, developed in the aftermath of Enron and other high-profile corporate scandals, have not changed significantly since then. They tend to focus more on reviews of internal controls and do not appear to fully reflect what are seen as some of the lessons of the more recent global financial crisis. For example, the OECD's review of lessons from the financial crisis found weaknesses in how companies approach risk management, recommending improvements in how companies link risks to business strategy, in establishing risk appetite frameworks, and in ensuring that risk receives due consideration by appointing a chief risk officer with a direct reporting line to the audit committee or board of directors. The absence of an internal auditor in 90% of listed Norwegian companies is also unusual in comparison to most developed markets. The Norwegian authorities consider that this can partly be explained by the fact that the average Norwegian listed company is relatively small in an international context.

Yet, whether Norwegian companies need to change their approach remains an open question. Interviews with management at a range of companies suggested that Norwegian companies have developed their own models for dealing with risk, usually based on the use of corporate risk management committees or risk officers who report to the CFO. They suggested that extensive attention is being given across all relevant categories of risk and presented regularly to the board in an integrated manner, and that the combination of management, audit committee and board scrutiny on risks leads to an effective establishment of risk appetites and risk limits that are well linked to overall corporate strategies, as well as steps to mitigate the most important risks.

At the same time, the significant decline in the number of public limited liability companies over the past decade and somewhat smaller recent drop in the number of listed companies suggest that both the benefits and costs of establishing new requirements for risk management in Norway should be considered carefully. For example, requirements for internal auditors or chief risk officers may have disproportionate impacts on smaller companies than on larger ones. Nevertheless, these questions merit further debate and consideration in the next review of Norwegian's Code of Practice for Corporate Governance.

Notes

1. See the Oslo Bors website 2012 figures on "shareholder structures" and "largest domestic companies by market value" on its Annual Statistics web page (*www.oslobors.no/ob_eng/Oslo-Boers/Statistics/Annual-statistics*).
2. This figure is cited in the Norwegian Ministry of Trade and Industry's 2010-11 Report to the Parliament (Storting) Summary, referencing data obtained from Oyvind Bohrend, "Eiren, styret og ledelsen. Corporate Governance i Norge" Fagbokforlaget 2011.
3. See *http://data.worldbank.org/indicator/CM.MKT.LCAP.GD.ZS/countries/NO?display=graph*.
4. These regulations are applicable to: 1) Financial institutions; 2) Regulated markets (i.e. stock exchanges); 3) Investment firms; 4) Management companies for securities funds; 5) Pensions

institutions; 6) Clearing houses; 7) Securities registers; 8) E-money institutions; 9) Insurance companies; 10) Estate agents; 11) Debt collection agencies; 12) External Accounting firms.

5. Interestingly, two of the other country Codes that do not directly recommend the use of internal auditor are in Denmark and Sweden, suggesting that this may reflect to some extent wider Nordic practice.
6. See *http://data.worldbank.org/indicator/CM.MKT.LDOM.NO*.
7. The Code also cites the relevant legal requirements from the Public Limited Liability Companies Act and the Accounting Act, which have already been cited earlier in this chapter.
8. See *www.lovdata.no/for/sf/fd/xd-20080922-1080.html* for the full text of the financial sector regulation on risk management and internal controls (Norwegian version; unofficial English translation provided by Google). Section 8 refers to separate requirements for disclosure. References to Section 9 address requirements for internal audit, while Chapter 4 addresses both internal audit requirements as well as alternative arrangements for those companies that do not have an internal auditor.
9. Section 6-41(2) of the Public Limited Liability Act exempts companies from establishing an audit committee that meet at least two of the following three criteria: i) average number of employees of less than 250, ii) a balance sum of less than NOK 300 million at the end of the accounting year, iii) a net turnover of less than NOK 350 million.
10. Operational risks, including those related to security, were also mentioned as an important consideration, for example in relation to a state-owned IT services company whose operational shut-down led to a failure of credit card payment systems to function for several days in 2011, leading to significant adjustments in its risk oversight framework.

Bibliography

Berzins, J., O. Bohren and P. Rydland (2008), *Corporate Finance and Governance in Firms with Limited Liability: Basic Characteristics,* Centre for Corporate Governance Research, Norwegian School of Management, *www.bi.no/ccgr*.

Crowley, K. (2011), "More Women Directors Will Improve Risk Management, ABI says", *Bloomberg News*, 27 September, *www.businessweek.com/news/2011-09-27/more-women-directors-will-improve-risk-management-abi-says.html*.

Deloitte (2012), *Deloittes CFO-undersokelse – Positive fremtidsutsikter.*

Ehling, P. (2008, revised 2013), *Corporate Insurance and Managers' and Owners' Risk Aversion*, Centre for Corporate Governance Research, Norwegian School of Management, *www.bi.no/ccgr*.

Ernst & Young (EY) (2012), *Corporate Governance 2012: Undersokelse av Arsrapporter for Regnskapsaret 2011, www.ey.no*.

European Confederation of Institutes of Internal Audit – ECIAA (2012), *Corporate Governance Codes on Internal Audit: Current Status in the EU.*

Folketrygdfondet (2012), *Ownership Report 2012*, *www.ftf.no*.

Folketrygdfondet (n.d.), *Management Mandate for the Government Pension Fund Norway*, *www.ftf.no*.

Fulton, L. (2013), *Worker Representation in Europe*, Labour Research Department and ETUI, *www.worker-participation.eu/National-Industrial-Relations/Countries/Norway/Board-level-Representation*.

Norwegian Corporate Governance Board (2012), *The Norwegian Code of Practice for Corporate Governance*, *www.nues.no*.

Norwegian Ministry of Trade and Industry (2011), "Active Ownership – Norwegian State Ownership in a Global Economy", *Meld. St. 13 (2010-2011) Report to the Storting (white paper) Summary*, *www.government.no*.

OECD (2013), *Size and Sectoral Distribution of State-Owned Enterprises*, OLIS document – DAF/CA/SOPP(2013)9.

OECD (2012), *Closing the Gender Gap: Act Now,* Chapter 15, Women on Boards.

Riksrevisjonen – Office of the Auditor General of Norway (2010), *Guidelines for Corporate Control*, *www.riksrevisjonen.no*.

Sjaafjell, B. and C. Kjelland (2010), *Corporate Governance: Country Report for Norway,* International Congress on Comparative Law, Washington 2010, *ssrn.com/abstract=1705665*.

Statoil (2013), "The In Amenas Attack: Report of the Investigation Into the Terrorist Attack on In Amenas", *prepared for Statoil ASA's Board of Directors*, *www.statoil.com/en/NewsAndMedia/News/2013/Pages/12Sep_InAmenas_report.aspx*.

Statoil (2012), *Annual Report*.

Statoil (2009), *Annual Report*.

Teigen, M. and V. Heidenreich (2010), "The Effects of the Norwegian Quota Legislation for Boards: Preliminary Findings", Norway Institute for Social Research (2010), *www.Boardimpact.com/PDF/MariTeigenogVibekeHeidenreich.pdf*.

UK Government (2011), *Women on Boards*, February, *https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/31480/11-745-women-on-Boards.pdf*.

Chapter 3

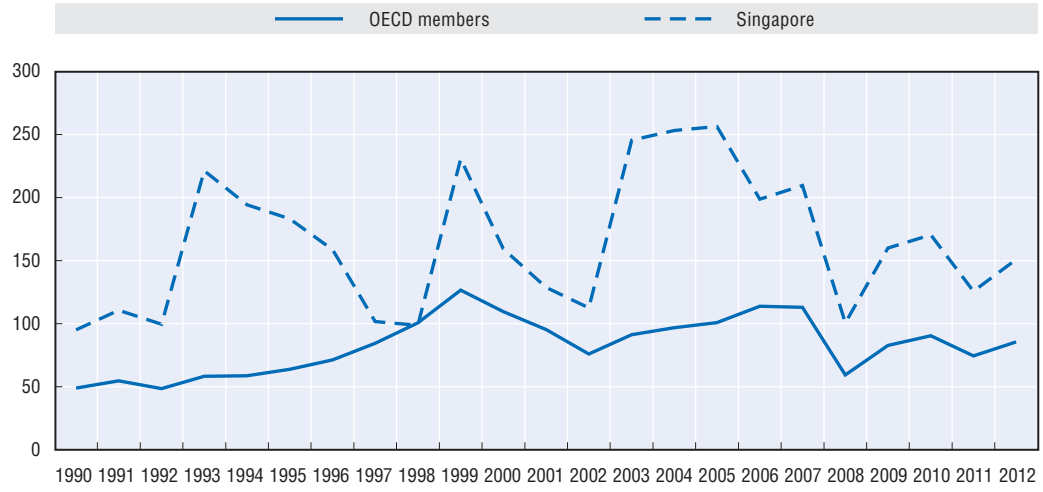
Singapore: The corporate governance framework and practices relating to risk management

This chapter, part of the sixth peer review based on the OECD Principles of Corporate Governance, *summarises the corporate governance framework and practices relating to corporate risk management in Singapore, with a focus on Singapore's recently adopted "Risk Governance Guidance for Listed Boards". The chapter was prepared by the OECD Secretariat (Akira Nozaki and Winfrid Blaschke).*

3.1. Introduction

Singapore has an active and diverse capital market for its size. The Singapore Exchange (SGX) maintains two boards, the SGX main board and the Catalist (formerly SGX-SESDAQ[1]). At the end of July 2013, the SGX had 782 listed companies with a combined market capitalisation of USD 1 233 billion (150% of GDP at the end of 2012).[2] Half of this is accounted for by the stock of top 30 listed companies included in the Straits Times Index. About 40% of SGX's listings are foreign, including regions such as Asia Pacific and further afield in Europe and the United States.[3] As a result, there is a significant diversity in the listing sectors which include real estate, shipping and offshore marine and infrastructure.

Figure 3.1. **Singapore – Market capitalisation (% of GDP)**

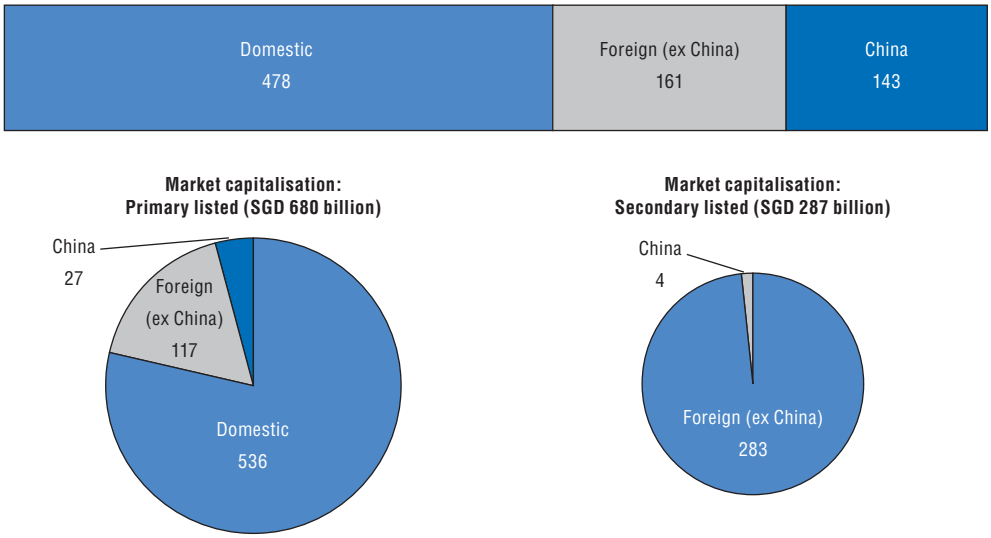


Source: The World Bank (n.d.), "Market Capitalisation of Listed Companies (% of GDP)", *http://data.worldbank.org/indicator/CM.MKT.LCAP.GD.ZS*.

The majority of listed companies in Singapore have a block shareholder holding of 15% or more shareholding.[4] The ownership structure comprises two main types; companies that originally started off as: i) family-owned businesses; and ii) state owned enterprises.[5] Ownership concentration has historically been high with families and the state representing major shareholders.[6] An important feature of the Singapore economic landscape is the presence of "government-linked companies" which are fully or partially state-owned. Temasek Holding (100% owned by the Singapore Ministry of Finance) holds a controlling share of some of the dominant companies in core industries, such as telecommunication, media, and transportation.[7]

Figure 3.2. **Singapore – Composition of the SGX listed companies (July 2013)**

Number of listed companies



Source: Singapore Exchange (2013a), *Market Statistics*, July, *www.sgx.com/wps/portal/sgxweb/home/marketinfo/market_statistics*.

3.2. Risk management standards and codes

Corporate governance framework

The regulatory framework for corporate governance in Singapore is underpinned by corporate law and securities regulations. These are reflected in common law rules as well as in statutory enactments such as the Companies Act, Securities and Futures Act, and Prevention of Corruption Act. This is supplemented by quasi-legislative enactments such as the SGX-ST Listing Manual, which applies to companies listed on the SGX.

A corporate governance code for listed companies ("Code") was first issued in 2001 and was revised in 2005. The Monetary Authority of Singapore ("MAS") issued a revised Code in May 2012, based on the recommendations submitted by the Corporate Governance Council[8] ("Council"). The Code is the main source of corporate governance principles and guidelines for listed companies in Singapore. The Code applies on a "comply or explain" basis; while the SGX Listing Manual requires listed companies (excluding those with a secondary listing) to describe in their annual report their corporate governance practices with specific reference to the Code. They must disclose any deviations from the Code and provide an appropriate explanation for the deviation in the annual report. These requirements are underpinned by the Securities and Future Act,[9] which makes the issuer corporation liable for breaches of the SGX's continuous disclosure rules.[10] Certain regulated industries such as financial institutions are subject to corporate governance regulations which are stricter than the "comply or explain" regime of the Code. Other non-statutory rules and guidelines include a guidebook for directors published by the Accounting and Corporate Regulatory Authority Singapore ("ACRA").

Singapore companies are becoming increasingly aware of the business practices for good corporate governance. Both the Securities Investors Association Singapore ("SIAS") and the Singapore Institute of directors ("SID"), which respectively represent minority retail investors and company directors, have participated in the process of improving

corporate governance standards.[11] They have also contributed to the implementation of these standards through conducting surveys and organising conferences. Currently, however, there is no formal mechanism for the regulator or the stock exchange to produce regular monitoring reports summarising how the Code is being followed in practice.

Risk governance guidance

The regulator and stock exchange in Singapore have recently taken a set of measures to enhance the risk management framework (Table 3.1). With effect from September 2011, the SGX updated the listing rules to bring into the continuing listing requirements both the need for adequate internal controls and an opinion from the board, with the concurrence of the audit committee, on the adequacy of the internal controls, addressing financial, operational, and compliance risks.

Table 3.1. **Singapore – Key measures of updating corporate governance framework**

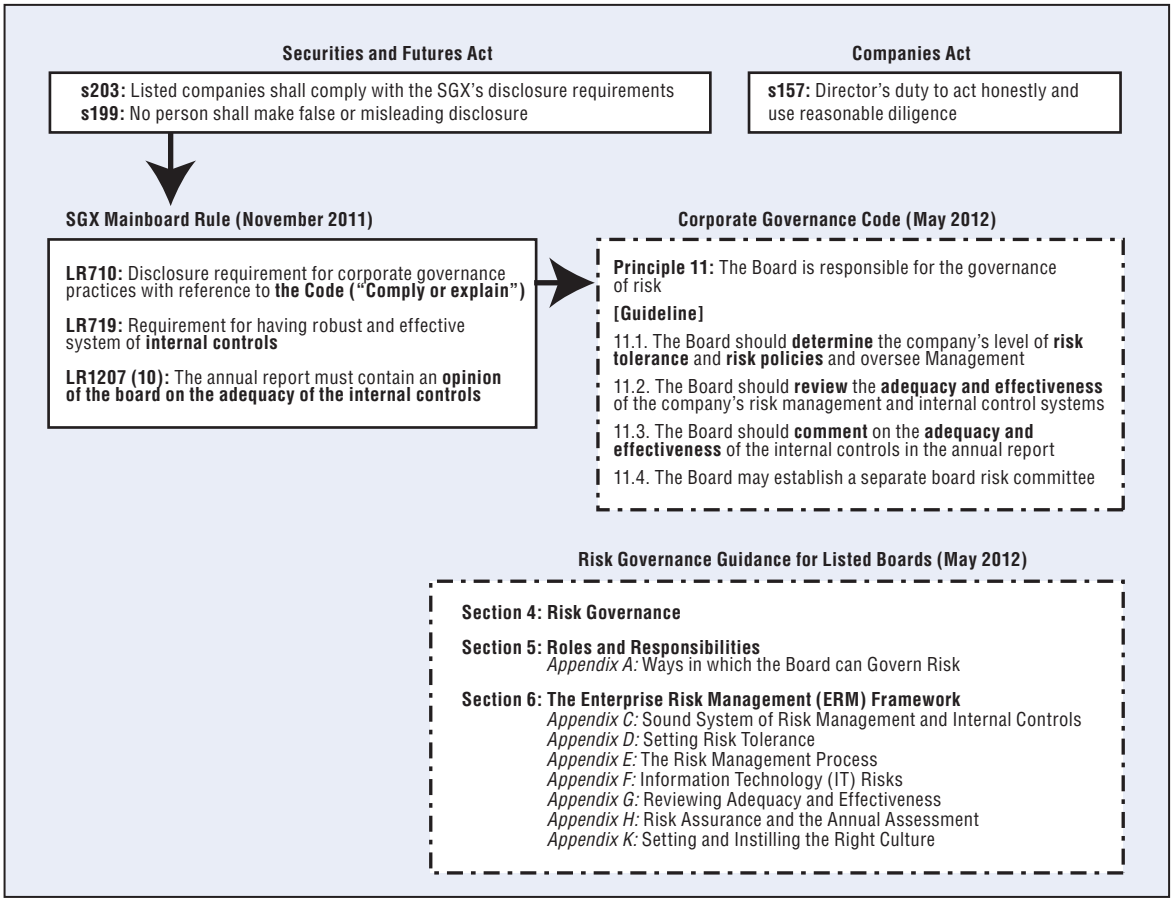
Date	Measure
March 2001	**The Corporate Governance Code** was first issued by the Corporate Governance Committee.
January 2003	**The Corporate Governance Code** entered into force. For general shareholder meetings held from 1 January 2003, listed companies are required to describe in annual reports their governance practices with specific reference to the Code.
July 2005	**The revised Code** ("2005 Code") was issued following the review by the Council on Corporate Disclosure and Governance.
October 2008	**The Guidebook for Audit Committees** was issued by the industry-led Audit Committee Guidance Committee.
July 2011	ACRA launched its first handbook for directors titled "**Being an Effective Director**".
September 2011	SGX updated **the listing manual** to bring into the listing requirements both the need for adequate internal controls and a specific opinion from the board on the adequacy of the internal controls.
April 2012	SGX issued an advisory note to all listed companies to provide guidance on compliance with the disclosure requirements on internal controls.
May 2012	MAS issued a revised **Code of Corporate Governance** ("Code") following a comprehensive review of the 2005 Code by the Corporate Governance Council ("Council"). The Code replaced the 2005 Code. Key issues addressed by the revised Code include: • The clarification of director independence and multiple directorships. [The Code clarified the definition of independent directors by requiring independence from substantial shareholders (10% shareholding) as well as defining a reference period for the length of term beyond which a director's independence should be revalidated (9 years).] • The enhancement of risk management and internal controls. • The enhancement of disclosure on remuneration practices.
May 2012	The Council issued a **Risk Governance Guidance for Listed Boards** ("Guidance") to provide further guidance on the board's role on risk governance *vis-à-vis* the Code.

The latest review of the Code in 2012 reflected the trend toward an integrated enterprise-wide perspective of risk management practices and the need to enhance board and management accountability for the company's risk management. Following the review of the Code, the Council in May 2012 released its *Risk Governance Guidance for Listed Boards* ("Guidance"), which acts as a complement to the Code. The Guidance provides key information on risk governance that the board should collectively consider when overseeing the risk management framework and policies. It also spells out the board and management's responsibilities in managing the risks.

The SGX's continuing listing requirements serve as a baseline to ensure that listed companies comply (or explain in cases of deviation) with risk management standards and codes. However, companies with a secondary listing on the SGX-ST (30% of total market capitalisation) are not required to comply with SGX-ST's continuing listing requirements as they are supposed to comply with the listing rules of their home exchange. It should be noted that there is a gap in this framework, as some countries (such as China and Vietnam)

do not have requirements or guidelines to disclose key risks in their annual reports.[12] The SGX only identifies on its website those companies that are not required to comply with its continuing listing requirements, without addressing the degree of equivalence between the SGX's requirements and the home exchange's requirements.

Figure 3.3. **Singapore – Overview of the regulatory framework for risk management**



3.3. The role of the board of directors

A key responsibility of the board is to ensure the soundness of risk management and to determine the firm's overall risk tolerance and risk policies.

Responsibilities of the board of directors

Companies must have a unitary board structure. The Singapore Code of Corporate Governance recommends a strong and independent element on the board, with independent directors making up at least one-third of the board (or at least half of the board under certain conditions such as the chair of the board and the chief executive officer being the same person). In Singapore's tightly-knit corporate community, appointing qualified independent directors is not a straightforward task, particularly in small and medium-sized enterprise segment, which comprises a large proportion of family-owned businesses.[13]

The Companies Act sets out a general requirement that directors shall at all times act honestly and use reasonable diligence in the discharge of the duties of their office.[14] The OECD (2010) states that the duty of reasonable diligence offers a way forward by making the board liable if assurance systems, such as risk management, are not in place. Enforcement against the violation of the duty of reasonable diligence is deemed feasible in Singapore. Even before the clarification by the amendment of the SGX listing rules in September 2011 that stipulated board responsibility for risk governance (Table 3.1), the board already had the responsibility for internal controls, including risk management, under the "comply or explain" framework.

The SGX has changed its approach towards board responsibility for risk governance from "comply or explain" to mandatory. With effect from September 2011, the SGX introduced a requirement to disclose in annual reports an opinion of the board, with the concurrence of the audit committee, on the adequacy of internal controls. The board is explicitly required to focus its attention in all three areas of risks, namely financial, operational and compliance risks. This framework is enforceable under the Securities and Futures Act, which prescribes that directors are liable for omissions and misleading or deceptive statements in disclosure documents.[15] This requirement has a significant impact on those companies where the board had delegated much of the work on internal controls and risks to the audit committee and/or risk committee.[16] In order to prevent listed companies from pursuing boilerplate statements in expressing the board's opinion, the SGX published an advisory note (Box 3.1.).

Box 3.1. **Singapore – Salient points from the SGX advisory note**

- There must be an opinion. Disclaimer or negative assurance such as "absence of evidence to the contrary" and the use of the words "believe" or "is satisfied" are not acceptable.
- Disclosure of opinion on internal controls must include "financial, operational and compliance risks".
- Opinion on internal controls should be formed at the Group's level instead of Company level only.
- Proper documentation should be maintained for the assessment of internal controls, addressing financial, operational and compliance risks.
- Factors considered and deliberated by the board and audit committee in arriving at the opinion should be disclosed.
- Areas of concerns or control deficiencies and remediation should be disclosed.
- Opinions should be disclosed in the Directors' Report or the Corporate Governance section of the annual report.

Source: Singapore Exchange (SGX) (2013b), "SGX-ST Listing Rules, Practice Note 12.2: Adequacy of Internal Controls", 2 April, *http://rulebook.sgx.com/net_file_store/new_rulebooks/m/a/MainBoard_April_2_2013.pdf*; Ernst & Young (2012), *Board Matters Quarterly*, Issue 12, June, Singapore, *www.ey.com/SG/en/Services/Assurance/Board-Matters-Quarterly---Issue-12---June-2012---Editorial*.

Board expertise

In order to fulfil their responsibilities, the Code recommends that boards comprise members with diverse background and skills, who as a group provide an appropriate balance and diversity of skills, experience, gender and knowledge of the company.[17] The

Code also highlights the importance of regular training for directors. The OECD (2010) recommended that the board develop a specific policy to identify the best skill composition of the board, possibly indicating the professional qualities whose presence may favour an effective board. To promote competent boards, it is also recommended that board members shall have access to training programmes, underpinned by periodic external board evaluations. The Singapore Institute of directors (SID), the largest national association of directors, has promoted the professional development of directors. SID organises conferences and provides training programmes for directors that address the recent trends including the update of the Code.

Succession planning

Succession planning for senior management positions is of critical importance and helps to lessen the influence of dominant personalities and behaviours.[18] The Code has addressed this issue by stating that nominating committees should make recommendations to the board on relevant matters relating to the review of board succession plans for directors, in particular, for the Chairman and the CEO. A study by KPMG and SMU (2009) revealed that succession plans for top management had not been given much priority. This became a critical risk factor for companies that did not have the key people in place for the future.

Board-level committees

The Companies Act requires that every listed company shall establish an audit committee ("AC"). The committee shall comprise at least three members, the majority of whom including the AC Chair shall be independent.[19] The Code further recommends that all of the members shall be non-executive directors.[20] The audit committee has an obligation under the Companies Act to review the external auditor's evaluation of the system of internal accounting controls. The 2012 Code also recommended that the audit committee shall extend its oversight to the company's internal controls, including financial, operational, compliance and information technology controls. Accordingly, risk related issues have traditionally been part of the audit committee's agenda, and many companies have relied on the audit committee to assist the board in its oversight of the company's risk management function.[21] The onus for ensuring that the company has effective internal controls addressing financial, operational and compliance risks still lies with the board but with the concurrence of the AC.

The establishment of a stand-alone risk committee is not mandatory for listed companies. Where risk committees exist, the Guidance requires the independence of the committee from management, and diversity of background and skill sets of committee members. One of the merits of having a stand-alone risk committee is to allow for more adequate risk oversight and give a formal voice to risk in strategic discussion. The risk committee can play the "second line of defence" and be separated from the audit function in the "third line".[22] One observation by the KPMG's survey shows that companies with a risk committee are often the most diligent at carrying out formal risk reporting (although there is a risk of having a false sense of security based on the frequency of reporting).[23] However, setting up a separate risk committee also has its downsides including: role of conflicts created among committees; danger of unlinking risks managed by different committees; lack of role clarity with senior management and department heads; too many committees; and not enough qualified directors.[24]

Each company has the discretion to establish a separate board-level risk committee, taking into account the capacity of the board and audit committee to review risk management. The Risk Governance Guidance recommends that due consideration be given to the factors which may affect their ability, including: the size and composition of the audit committee; the scale, diversity and complexity of the company's operations; and the nature of significant risks faced. Setting out a clear division of the roles of an audit committee and a risk committee in an effective manner is one of the challenges, particularly for companies which have recently established a risk committee. While the legal and regulatory framework has already attributed many of the risk management related tasks to the audit committee, there is little guideline on how a risk committee fits into the framework. Apart from this, many of the aforementioned downsides of having a risk committee can be managed by enhanced communication between the risk, audit and other relevant committees. Indeed, the Guidance underlines the importance of communication among committees.

3.4. Structure and organisation of the risk management system

Enterprise-wide risk management (ERM)

There is an increasing tendency toward an integrated or holistic view of risks. Nearly half of the surveyed companies[25] indicated that they had already implemented an enterprise-wide risk management (ERM) programme. The majority of the remaining companies had planned to implement an ERM programme by the end of 2013.[26] One-third of the companies with an ERM programme have not defined their organisation's risk appetite.[27] The KPMG's survey observes that most companies with an ERM programme have not integrated all associated risk-related functions to achieve a dashBoard view of the risks on an enterprise-wide basis. The SID and SGX set out the following as the most challenging factors hindering the identification and management of enterprise-wide risk: risk factors relating to people;[28] necessary level of investment; and availability and timeliness of information (SID and SGX, 2011).

The Risk Governance Guidance gives a summary of the ERM process, referring to COSO's definition.[29] It describes common characteristics containing: i) risk strategy and risk policy; ii) risk management process; and iii) organisation structure, culture and people, and technology and tools. While the Guidance refers to its applicability to small and medium-sized enterprises (SMEs), it does not further elaborate on how to implement cost-effective internal controls and risk management for SMEs.[30]

Chief risk officers (CROs)

While the appointment of a Chief Risk Officer (CRO) is becoming prevalent in large companies,[31] it is not specifically recommended in the Risk Governance Guidance in Singapore. The role of CROs is articulated in the Guidance as providing executive oversight and co-ordination of the company's risk management efforts.[32] The OECD (2010) recommends that "the CRO or equivalent should be able to report directly to the board along the lines already advocated in the OECD Principles for internal control functions reporting to the audit committee or equivalent". While some companies have ensured a direct reporting line from the CRO to the chair of the Board-Level Risk Management Committee, the Guidance does not recommend establishing robust communication and reporting procedures between the board and CRO.[33]

The reality is that CFOs are operating as *de facto* CROs in many companies especially in SMEs. However, many observers view this practice negatively, pointing out that the

involvement and influence of the CFO in many of the core tasks (e.g. budgeting, financial reporting[34] and performance management) may conflict with the CRO's role in the oversight of risk management practices.[35]

Whistle-blowing policy

The Code attributes the responsibility for reviewing a whistle-blowing policy to the audit committee. The whistle-blowing policy shall ensure that concerns about possible improprieties are raised and independently investigated, and appropriate follow-up action is taken. The Code also recommends that the existence of the policy and its procedure is disclosed in annual reports. The survey of 68 listed companies conducted by the SID and SGX showed that 95% of companies have a whistle-blowing policy in place to allow employees and others to raise concerns about possible improprieties. One third of these companies disclosed policy details in annual reports and did not disregard anonymous complaints (SID and SGX, 2011). Singapore has not introduced specific legislation in relation to whistle-blowing. Providing adequate protection, including legal safeguards and institutional assistance to whistle-blowers in companies,[36] has now become an issue in some jurisdictions.

Information processing

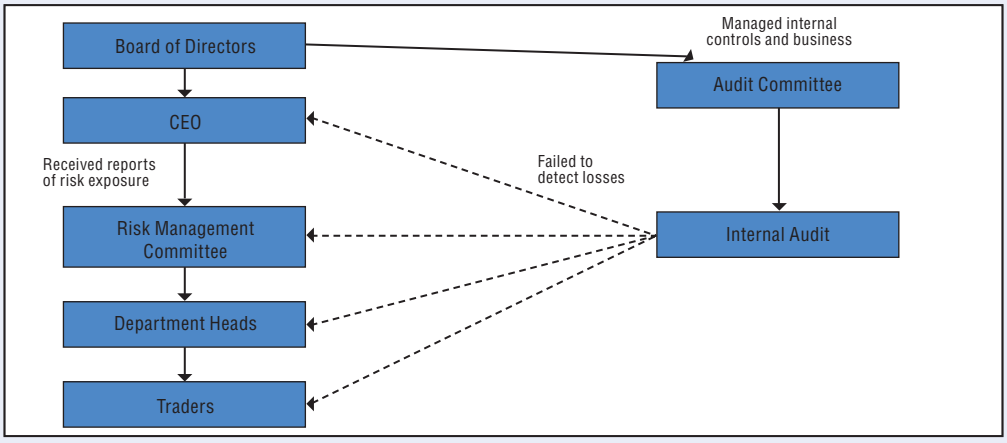
Encouraging the board to exercise an informed judgment[37] is essential to all areas, including risk management. While listed companies have appointed an increasing number of independent directors, those are often left out of the loop of information on material issues, and sometimes it is too late for them to react appropriately when they have the relevant information (see the case of China Aviation Oil Corporation in Box 3.2). The annotations to the OECD Principle VI.D.7 note that "ensuring the integrity of the essential reporting and monitoring systems will require the board to set and enforce clear line of responsibility and accountability throughout the organisation". Taking into account that the board (especially independent directors) have no control over information supply in practice, it is essential to establish a governance structure that ensures independent directors have access to timely and relevant information without any interference by executive directors and management. The Code and Guideline have implemented several recommendations addressing communication between the board and management.[38] It may be worth considering that the CRO meet periodically with directors without executive directors and management present.[39]

Box 3.2. **Singapore – The case of China Aviation Oil Corporation Ltd.**

China Aviation Oil Corporation Ltd. (CAO) is the Singapore subsidiary of China Aviation Oil Holding Company (CAOHC), one of the largest state-owned enterprises in China. CAO practically handled 100% of China's jet fuel imports for civil aviation. CAO went public and was listed on the SGX main board in 2001. CAO was acknowledged for its outstanding risk management structure and procedures by China National Enterprise Federation at its 10th annual creative management awards. The company was in the spotlight in November 2004 when it announced that it was not able to meet some of the margin calls arising from derivative trading. The company sustained losses of up to USD 550 million as a result of unauthorised speculative options trading in fuels and was on the brink of collapse. The company's CEO was arrested on charges of insider trading in March 2006.

In March 2003, the company's management had entered into speculative fuel options trading with the aim of seeking profits from market movements. This was beyond the remit authorised by the board whereby the company should use derivatives as a hedging instrument to hedge against risks inherent in its primary business of physical oil

Box 3.2. **Singapore – The case of China Aviation Oil Corporation Ltd.** *(cont.)*



procurement and trading. There was no risk management policy to govern options trading. Despite early successes, trade losses began to accumulate when oil price movements went against the company's trading strategy. The CEO manipulated the accounts and did not report the losses in the company's financial statements. Just before CAO sought court protection in November 2004, CAO had not provided any relevant information for its independent directors, external auditors, or regulators. CAOHC sold 15% of its stake in CAO to investors through a private placement at the time when it possessed non-public information regarding the losses in CAO.

The investigations by the Commercial Affairs Department and PwC discovered severe lapses in corporate governance and disclosure practices by both CAO and CAOHC. They revealed that CAO overrode risk controls and the description of the risk management practices in the annual report was not consistent with the actual risk management practices. Identified weaknesses are summarised as follows: i) some of the directors had recognised that CAO was speculating in options but no proper action had been taken; ii) no effective risk management guidelines in practice on options trading; iii) board of directors allegedly not aware of losses incurred; iv) audit committee and internal audit did not detect losses.

The CEO and head of finance were convicted and sentenced to 51 months and 24 months of imprisonment, respectively. Other directors were fined for making false and misleading statements. CAOHC knew of the losses at its subsidiary and had to pay a civil penalty of USD 8 million to the MAS under Section 232 for breaching the insider trading provisions of the Securities and Futures Act.

Securities Investors Association of Singapore (SIAS) played a significant role in guiding retail investors of CAO. In December 2004, SIAS recommended shareholders not to take legal actions against CAO that was already under water. Mr. Gerald, President/CEO of SIAS said, "CAO had few assets to sell to raise money. Even if shareholders succeeded in getting judgment against the company, it would be just a paper judgment. And the Chinese would have gone away to restart their business elsewhere…" Against SIAS's recommendation, three class action suits were filed in the United States, but they were rejected over jurisdiction.

In January 2005, SIAS held a meeting with the government of China to restructure CAO. The President of CAOHC assured SIAS that the scheme of arrangement demonstrated CAOHC's goodwill and sincerity in finding an equitable solution.

Source: Teik, L.C. (2009), "Dare to Challenge! The SIAS Story", *Straits Times Press*; Teen, M.Y. (2006), "Implementation and Enforcement of Rules in Singapore and the Case of China Aviation Oil", presented at the 2006 OECD Asian Roundtable, *www.oecd.org/daf/ca/corporategovernanceprinciples/37997933.ppt*; Tijo, H. (2009), "Enforcing Corporate Disclosure", *Singapore Journal of Legal Studies*, 332-364, *http://law.nus.edu.sg/sjls/articles/SJLS-Dec09-332.pdf*.

3.5. Risk management policies

The enterprise-wide risk management policy helps establish a structured and disciplined approach towards managing risk in the organisation's core business processes and decision-making activities. The Guidance enumerates the key elements that a risk management policy should contain.[40] One of the elements is the details of procedures for risk recognition and ranking (risk assessment). The existence of clear terminology for defining and interpreting risk is an essential element to share the common risk management policy at an enterprise-wide level. Without a well-recognised common risk language, a risk management policy could end up as a facade. The SID and SGX survey showed that 98% of the companies have a risk management policy, but only 27% of them adopted a common terminology and set of standards to manage risks. Above all, sharing the same understanding of key risk factors within the company from the front-line employees to the top management is an essential factor to ensure the implementation of the risk management system.

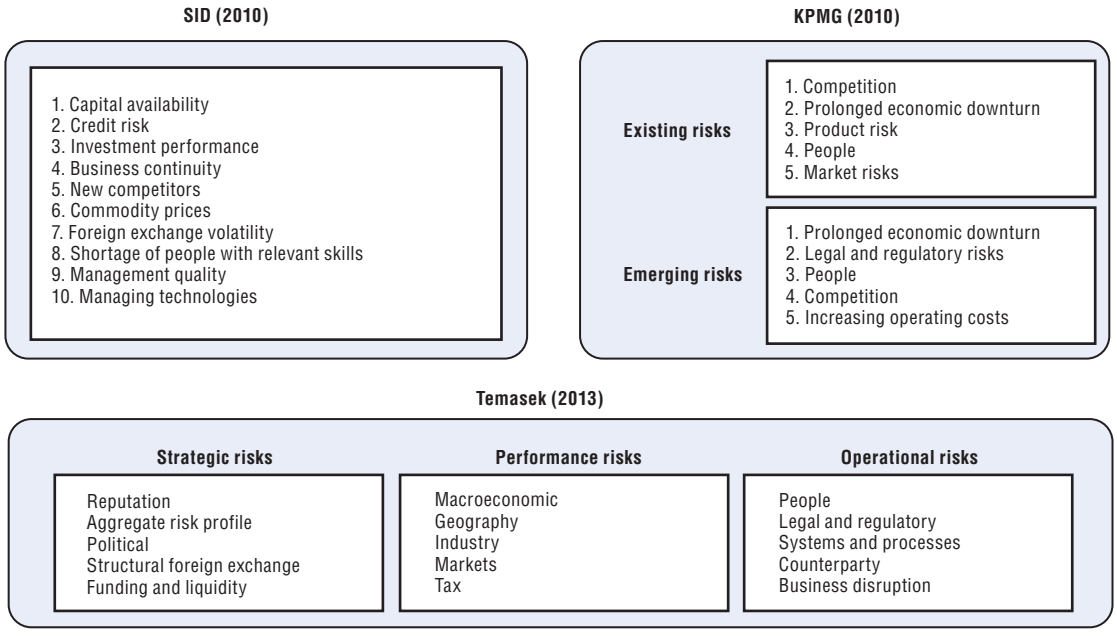
Examples of key risk factors identified by Singapore firms and Temasek are illustrated in Figure 3.4. Temasek Holdings, which has a majority or full ownership on some of the largest firms in core industries, covers three categories of risk in its risk management framework. The firm's business models are usually reflected in the recognition and ranking of the key risk factors.[41] Consequently, the companies tend to focus on the risks to which they are accustomed in their daily operations, with their risk management systems usually failing to identify catastrophic risks with occasional severe losses (fat tails) and dependence.[42] For instance, the 2013 smoky haze due to illegal burn off in nearby Sumatra wreaked havoc on the Singapore economy.[43] Marsh Risk Consulting pointed out that "while many firms have procedures or plans for emergencies that impact on business continuity and/or crisis management, they may not adequately cover a situation such as prolonged periods of haze affecting employees and the general population on a wide scale".[44] As the risks facing each listed company will differ according to a number of factors,[45] the regulators and stock exchange consider that it may not be practical to periodically identify country-wide characteristics of risk concentration, complexity and interconnectedness, or provide guidance on selected types of risk that will apply to all countries.

The SGX considers that a risk management approach that incorporates sustainability issues provides management with useful data for identifying emerging issues. The SGX in its *Guide to Sustainability Reporting for Listed Companies*[46] sets forth a Principle stating that sustainability reporting (which provides an account of the company's consideration and performance of environmental, social and governance issues) "allows listed companies to consider emerging risk areas and to identify opportunities presented by risks that are overlooked by other analytical and systems driven approaches".

Risk appetite and risk tolerance

The Singapore Code of Corporate Governance and Risk Governance Guidance recommends that the board determines the company's levels of risk tolerance and risk policies (sometimes termed risk appetites[47]). Further instructions are provided in the Guidance with regard to how the risk tolerance can be set in the company. The annotations to the OECD Principle VI.D.1 note that risk policy (risk appetite) is closely related to strategy and "will involve specifying the type and degree of risk that a company is willing to accept in pursuit of its goals. It is thus a crucial guidance for management that must manage risks to

Figure 3.4. **Singapore – Key risk factors identified by listed companies and Temasek**



Source: Singapore Institute of directors (SID) and Singapore Exchange (SGX) (2010), *Singapore Board of directors Survey 2010*, available at: *www.sid.org.sg/web_surveys_awards/Board_survey*; KPMG (2010), "Charting a Safe and Sustainable Growth Journey: Singapore Enterprise Risk Management Survey 2010", available at: *https://www.kpmg.com/SG/en/IssuesAndInsights/ArticlesPublications/Documents/SgERMSurvey2010.pdf*; Temasek (2013), *Review 2013*, available at *www.temasekreview.com.sg*.

meet the company's desired risk profile". The Institute of Risk Management distinguishes between the risk appetite and risk tolerance.[48] Risk tolerance is deemed as one of the elements that affect the determination of risk appetite. It also represents the application of risk appetite to specific objectives.[49] Taking the interaction between risk appetite and risk tolerance into account, it is important to articulate and communicate an enterprise-wide risk appetite in alignment with risk tolerance.[50] However, the Guidance does not clearly address the interaction between the risk policy (risk appetite) and risk tolerance.

Risk appetite and risk tolerance shall be calibrated on a periodic basis and be responsive to new business strategies and a changing market environment. External inputs are particularly useful in this process. They can provide insights into market conditions, emerging international trends and evolution in best risk management practices, helping the board to regularly upgrade its fact-base and challenge its own and the institution's "conventional wisdom".[51] Many of the board members and executives in Singapore are keen on sharing up-to-date risk information through the communication platform such as conferences held by SID.

Risk and culture

Risk management is inexorably linked to the organisation's culture. The Guidance addresses the importance of setting and instilling the right culture, by emphasising that "good culture results in better judgment, which reduces the reliance on process and provides greater comfort to the board and management". In order to test if a risk culture pervades in the organisation, some observers in Singapore emphasise the importance of asking for the "top 3 priorities of business strategies" and "top 3 risk profiles" to the board and management as well as risk-taking staff. Besides the risk appetites and risk profiles, it

is also important that all risk-taking staff recognise the amount of risk their actions adds, what their limits and tolerances are, and what the consequence are of breaching these ("front-line risk culture initiatives").[52]

There is a need to consider the cultural differences between countries where companies are operating, particularly in Singapore where foreign companies account for a large part of listed companies. These cultural differences may make it difficult for the headquarter to determine an ERM framework that is applicable in different jurisdictions.[53] One of the elements that describe the cultural differences in relation to risk management is the extent to which corruption is believed to exist. The OECD (2011)[54] highlights that Singapore marked 9.2 (scale of 0 to 10) on the corruption perception index, the second highest score in terms of perception of corruption in Asia Pacific and higher than most of the OECD countries (OECD average: 7.0).

3.6. Independent assessment of the risk governance framework

A risk governance framework requires on-going maintenance, including a periodic calibration of risk appetite and risk tolerance. Independent assessments of the framework play an essential role in its on-going maintenance, and this may involve internal parties, such as internal audit, or external resources such as audit firms and consultants.[55]

Internal audit

The annotations to the OECD Principle VI.D.7 state that one way of ensuring the integrity of the essential reporting and monitoring system (including systems for risk management) is through an internal audit system directly reporting to the board. The Risk Governance Guidance in Singapore is in line with the annotations, stating that the board's annual assessment should consider, where applicable, the work of its internal audit function and other providers of assurance.[56] It is estimated that about one-third of listed companies in Singapore do not have a full time internal auditor.[57] Securities Investors Association of Singapore (SIAS) and other institutions have suggested that all listed companies reinforce internal audit, and appointments and resignations of internal audit executives be announced to the SGX.[58] The role of internal auditors is expected to be crucial, as the new SGX regulation and the Code raised the board's risk management responsibilities.[59]

External auditors

There is no statutory requirement that listed companies have their internal control system (including risk management) regularly audited by external auditors. However, in addition to issuing an audit report, Singapore's Accounting and Corporate Regulatory Authority expects that a good audit will uncover issues and learning points that are useful for a company, including the improvement of risk management, the strengthening of corporate governance and the challenging of underlying business assumptions.[60] The Companies Act attributes the responsibility for nominating and reviewing the external auditor to the audit committee. The audit committee may consider the auditor to be one of its "lines of defence" in overseeing the quality and integrity of the risk management function.[61]

Statutory auditors have a duty to be alert to the possible existence of fraud, and to discharge their obligations with reasonable care. Singapore courts have addressed the duty of auditors in recent cases by clarifying the law of professional negligence (Box 3.3). The appeal court clearly states that auditors shall verify and be sensitive to the possibility of fraud.

Box 3.3. **Singapore – The court decisions on the duties of statutory auditors**

Case 1: PlanAssure PAC vs. Gaelic Inns Pte Ltd. [2007] SGCA 41

The auditor (PlanAssure PAC) was engaged by the company (Gaelic Inns Pte Ltd.) to audit the company's accounts for FY 2001, 2002 and 2003. Between 2001 and 2004, the former manager at the company devised and carried out a "teeming and lading" scheme, whereby she delayed banking in cash on the day of sales into the respondent's bank account, and instead used the cash for her personal benefit. The misappropriation of funds (USD 1 m in total) was not detected by the auditor due to a failure to appreciate the significance of large sums of cash in the company's accounts.

The company commenced the suit against the auditor, in which it sought damages for negligence in respect of the audits performed between 2002 and 2004. The auditor appealed against the trial judge's decision and raised issues including whether the respondent had been contributory negligent. The salient points of the decision by appeal court are:

- The auditor, in failing to recognise, from the striking facts before it, that something was amiss, had failed to comply with the standard of care which could reasonably be expected of it in the circumstances. If the auditor had exercised due care in its audit and detected the fraud, the company would promptly have taken the necessary steps to investigate the misappropriations.
- Contributory negligence could arise if the company was found to have failed to look after its own interests even though it had appointed an auditor. The cumulative lapses on the part of the company's directors constituted serious management failure and ought to be treated as fault for the purposes of a defence of contributory negligence.

Source: Singapore Law Reports (2007a), "PlanAssure PAC (formerly known as Patrick Lee PAC) vs. Gaelic Inns Pte Ltd. [2007] 4 SLR(R) 513; [2007] SGCA 41", *www.singaporelaw.sg/sglaw/laws-of-singapore/case-law/cases-in-articles/negligence/1607-planassure-pac-formerly-known-as-patrick-lee-pac-v-gaelic-inns-pte-ltd-2007-4-slr-r-513-2007-sgca-41*.

Case 2: JSI Shipping Pte Ltd. vs. Teofoongwonglcloong [2007] SGCA 40

The company (JSI Shipping Pte Ltd.) engaged the auditor (Teofoongwonglcloong) to conduct three statutory audits of the company. All three audits were unqualified. The company sustained losses as a result of its Asia director ("Riggs") siphoning off its funds by misstating his remuneration.

The company brought an action against the auditor for damages resulting from alleged breaches of its contractual obligations and duty of care in auditing the company's accounts. The company alleged that the auditor had failed to adequately verify Riggs' entitlement to remuneration despite having become aware of the need for such objective verification. The auditor claimed that it was entitled to rely on the signature of the other director ("Cullen") on the draft financial statements as verification of Riggs' remuneration. The salient points of the decision by appeal court are:

- The auditor failed to comply with the standard of care by not: a) making proper or further inquiries; b) seeking assurance or verification of Riggs' remuneration; nor c) carrying out any appraisal of the system of oversight and control exercised by the company. The essence of an audit was to obtain and provide reasonable assurance that a company's accounts provided a true and fair view of the financial position of the company. This encompassed the duty to verify and to be sensitive to the possibility of fraud.
- The fault was attributed equally to both the auditor and the directors of the company, as they were just as negligent and had not discharged their responsibilities according to good corporate governance.

Source: Singapore Law Reports (2007b), "JSI Shipping (S) Pte Ltd. vs. Teofoongwonglcloong (a firm) [2007] 4 SLR(R) 460; [2007] SGCA 40", *www.singaporelaw.sg/sglaw/laws-of-singapore/case-law/cases-in-articles/negligence/1606-jsi-shipping-s-pte-ltd-v-teofoongwonglcloong-a-firm-2007-4-slr-r-460-2007-sgca-40*.

Under the Singapore Companies Act, an auditor has a mandatory duty to report to the authority if they have reason to believe that a serious offence involving fraud or dishonesty is being or has been committed against the company by officers or employees of the company. This requirement does not appear to cover suspected accounting fraud. In the reviewing process of the Companies Act in 2013, the Ministry of Finance agreed that the scope of this requirement shall not be expanded to include suspected accounting fraud as: i) in practice, it is difficult for an auditor to determine from the circumstances of a misstatement whether there is a case of accounting fraud or if it was just an honest mistake; and ii) in any case, auditors are already required in law to deal with material misstatements detected in accounts by the relevant disclosures in the accounts and to the Registrar of Companies (if applicable).[62] However, the framework of mandatory reporting to the regulator may exert greater pressure on the company to promptly remedy the misstatement, if it is further elaborated.[63]

3.7. The role of shareholders

Institutional shareholder activism is fundamental in raising corporate governance practices. A survey by ACCA and SIAS (2011) revealed that most investors are seeking more information from companies about their risk management including the board's opinion.[64] Nevertheless, challenges exist with regard to the disclosure of corporate strategy and business models which tend to be boilerplate in nature.[65] Major issues still remain in the area of risk reporting such as how to discourage boilerplate reporting without having to establish safe haven rules.[66] One noteworthy approach in Singapore is enhancing communication with stakeholders through sustainability reporting, although the concerns about boilerplate still remain. While not mandatory, listed companies are encouraged to consider sustainability reporting as an integral part of good corporate governance. The SGX considers that the report can be used for benchmarking and assessing sustainability performance, demonstrating how the company influences and is influenced by expectations about sustainable development and facilitate peer comparison over time.[67]

There is a perception that particularly in a small economy like Singapore it may be the regulator, through the use of civil penalties, that is the most cost efficient and effective enforcer of securities laws rather than the investors themselves or any self-regulatory organisation.[68] Tjio (2009) discusses that "in any case, since the contravening person for the purposes of the continuous disclosure rule is the issuer company itself, which may not have made a profit or avoided a loss from failure to disclose material information unless it was also issuing new shares at the same time, investors will usually be unable to recover anything at all". While shareholders can sue on behalf of a company, the legal framework of derivation actions embraces some weaknesses including that shareholders are unable to claim legal costs from the company or have access to company documents. In consequence, due to the structure of the legal framework, investors may find it costly and hence not worthwhile to initiative civil actions.

Under these circumstances, SIAS has played a leading role in resolving issues between shareholders and listed companies. Having a former judge as the President, SIAS maintains the stance: "In the boardroom and not the courtroom." Instead of prompting minority shareholders to file a lawsuit, SIAS seeks an alternative approach mainly through informal meetings to facilitate communication between shareholders and the boards of listed companies. SIAS sometimes acts as a representative of minority shareholders and negotiates with the listed companies (see the case of China Aviation Oil Corporation in

Box 3.2). While this approach can save on enormous amount of money and time, it is not easy to find a qualified person to take this role, which requires expertise on a wide range of corporate affairs as well as the confidence of both shareholders and boards.

3.8. Conclusions

Regulators and market participants (both investors and boards of listed companies) are keen to enhance corporate governance standards, to increase the attractiveness of the capital markets. This is reflected by recent developments in the area of risk governance, through the update of listing requirements and Corporate Governance Code as well as the publication of a Risk Governance Guidance. This Guidance, which covers many relevant issues and contains a number of examples to facilitate its implementation, is deemed as one of the most comprehensive national guidelines in the area of risk governance. In this respect, Singapore seems to have strived for addressing the challenge highlighted in a report prepared for the OECD (Anderson, 2010), which states that "Most of the guidance […] gives scant guidance on how to create an effective risk management and assurance". Although some areas of improvement, both in the contents and implementation of these standards, remain, it is expected that regulators and market participants will take appropriate measures toward their further development.

Against this background, as the Guidance is relatively new, actual practices with regard to the implementation of the new risk governance framework have yet to be observed. It also remains to be seen how the new provision in the listing rule prescribing the board responsibilities for risk governance can effectively be enforced by regulators or through civil procedures. Most importantly, risk governance systems should be capable of adapting to differences in risk culture, particularly in Singapore where foreign companies account for a large part of listed companies. Regulators and market participants are well aware of the importance of setting and instilling the right culture. Risk governance practices under Singapore's new framework, which may become a benchmark for other jurisdictions, shall closely be monitored.

Notes

1. SGX-SESDAQ was established in 1987 to enable companies that did not meet the criteria for SGX main board listings to raise money from the public.
2. 645 companies in the SGX main board and 137 companies in the SGX Catalist.
3. At the end of July 2013, 39% of the listed companies (45% of their total market capitalisation) are foreign and 47% of the foreign companies (7% of their total market capitalisation) are Chinese. See SGX (2013).
4. See Tan (2006).
5. See Yeo et al. (2002).
6. See Claessens, Djankov and Lang (2000).
7. Temasek Holdings directly owns majority shares in the following enterprises: Financial Services (67% of PT Bank Danamon Indonesia, Tbk) Telecommunications, Media & Technology (100% of Singapore Technologies Telemedia Pte Ltd., 84% of STATS ChipPAC Ltd., 100% of MediaCorp Pte Ltd., 52% of Singapore Telecommunications Limited), Transportation & Industrials (66% of Nepturne Orient Lines Limited, 100% of PSA International Pte Ltd., 56% of Singapore Airlines Limited, 100% of Singapore Power Limited, 54% of SMRT Corporation Ltd.), Life Sciences, Consumer & Real Estate (100% of Mapletree Investments Pte Ltd., 60% of Surbana Corporation Pte Ltd., 88% of Wildlife Reserves Singapore Pte Ltd.). See Temasek (2013).

8. The Corporate Governance Council had the role to seek for promoting a high standard of corporate governance in companies listed in Singapore. The Monetary Authority of Singapore (MAS) appoints the members of the Council. Members of the Council are drawn from the business community and stakeholder groups, and have been appointed for a two-year term. Representatives from MAS, the Accounting and Corporate Regulatory Authority (ACRA) and Singapore Exchange Limited (SGX) are appointed to the Council on an ex-officio basis. See MAS (2010).
9. Section 203 of the Futures and Securities Act prescribes that the SGX listed companies "shall not intentionally, recklessly or negligently fail to notify the securities exchange of such information as is required to be disclosed by the securities exchange under the listing rules or any other requirement of the securities exchange".
10. The criminal sanctions for the market misconduct provisions are a fine of up to USD 250 000 and imprisonment of up to seven years.
11. In practice, SIAS and SID are often consulted for their views before implementation of key regulatory frameworks affecting investors and directors. See Yip and Tan (2011).
12. See Irving Low (2012).
13. See Irving Low (2012).
14. Section 157(1) of the Companies Act. In the Companies Amendment Bill 2013 for consultation (ended on 14 June 2013), it is not proposed to revise the provision of Section 157(1).
15. Section 199 of the Securities and Futures Act. Section 204(1) prescribes that the penalty of contravening this provision is a fine not exceeding USD 250 000 or to imprisonment for a term not exceeding seven years or both.
16. Delegation of duty is not a breach but allowed under the Companies Act. Section 157C of the Companies Act states that a director may rely on information prepared by any other director or any committee of directors upon which the director did not serve in relation to matters within that other director's or committee's designated authority. This shall apply to a director only if the director: a) acts in good faith; b) makes proper inquiry where the need for inquiry is indicated by the circumstances; and c) has no knowledge that such reliance is unwarranted.
17. The FSB (2013) recommends that "the board needs to comprise members who collectively bring a balance of expertise, skills, experience and perspectives while exhibiting the objectivity to ensure decisions are based on sound judgement and thoughtful deliberations".
18. See FSB (2012).
19. Companies Act 201B(2) requires that a majority of the members shall not be non-executive directors of the company or any related corporation. The Guideline 12.1 of the Code recommends that a majority of the members shall be independent.
20. This is supported by the ACGC (2008) arguing that the presence of the CEO as a member may compromise the committee's objectivity and ability to exercise independent judgment. The ACGC was established by the Monetary Authority of Singapore (MAS), the Accounting and Corporate Regulatory Authority (ACRA), and the Singapore Exchange Ltd. (SGX) in January 2008.
21. See Appendix A2.1 and 2.2 of the *Risk Governance Guidance*.
22. See Pederson and Cheng (2012).
23. 78% of the companies with a board-level risk committee organise monthly or quarterly reporting, while this figure is 45% for the board and audit committees (KPMG, 2010).
24. See Choi (2013).
25. 51% of the companies (203) surveyed by KPMG (2010), 46% of the companies (68) surveyed by SID and SGX (2011).
26. 27% of the companies surveyed by KPMG (2010).
27. 29% of the companies surveyed by KPMG (2010).
28. 56% of the surveyed companies by SID and SGX (2011) reported the lack of risk-trained people as a challenging factor.
29. ERM 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 tolerance, to provide reasonable assurance regarding the achievement of the entity's objectives" (COSO, 2004).

30. Mak Yuen Teen (2007) stated, "COSO has recently published guidance for smaller companies on internal control over financial reporting. Although this is targeted at smaller US companies in applying s404 and focuses on internal control over financial reporting, it may nevertheless be useful as a source for developing similar guidance for Singapore companies."

31. In some of the surveyed companies, the head of the risk management department functions as a CRO.

32. The CRO in a SGX listed company described, "The definition of a CRO is very loosely-interpreted" and "CROs in the financial sector have different responsibilities and authority". She described the CRO's role as "more of a risk coordinator and adds value by providing advice on industry trends for management to consider during quarterly reporting". See Singapore CFO Institute and PwC (2013).

33. The MAS issued additional guidelines on corporate governance for financial institutions in April 2013. While appointing a CRO is not mandatory, it is required that the CRO should have a reporting line to the board or board risk committee and have the right to seek information and explanations from senior management.

34. The Audit Committee Guidance Committee (ACGC) guidebook advocates that the CEO and CFO should sign an undertaking confirming their responsibilities for internal controls in relation to the financial reporting. Guideline 11.3 of the Code state that the board should also comment in the company's Annual Report on whether it has received assurance from the CEO and CFO with regard to the proper maintenance of the company's financial records and the effectiveness of the company's risk management and internal control systems.

35. See Singapore CFO Institute and PwC (2013).

36. With regard to public officials, as of 2009 almost 90% of all OECD member countries provide some sort of protection to whistle-blowers, most often legal. Several countries provide anonymity and others protect whistle-blowers against dismissal or other forms of retaliation (OECD, *Government at a Glance*, 2009). See also OECD, "Whistle-Blower Protection: Encouraging Reporting", July 2012.

37. One of the recommendations made in the Kay Review (2012) is that "regulators should avoid the implicit or explicit prescription of a specific model in valuation or risk assessment and instead encourage the exercise of informed judgment".

38. Under the Code, companies are required to provide information to directors on a timely basis. Principle 6 states that directors should be provided with complete, adequate and timely information prior to board meetings and on an on-going basis. Guideline 10.3 goes on to state that management should provide all members of the board with management accounts and such explanation and information on a monthly basis. In addition, Guideline 12.5 also suggests that the audit committee should meet a) with the external auditors, and b) with the internal auditors, in each case without the presence of Management, at least annually.

39. FSB (2013) recommends "ensuring the CRO has unfettered access to the board and risk committee (including a direct reporting line to the board and/or risk committee), and expecting the CRO to meet periodically with directors without executive directors and management present".

40. The Risk Governance Guidance in Singapore follows a structured approach to ERM and the requirements of ISO 31000 (Institute of Risk Management, 2010), covering the following elements: governance; risk strategy; risk culture and control environment; risk tolerance; risk architecture; risk assessment; risk protocols; risk response; allocation of roles and responsibilities; training topics and priorities; monitoring and benchmarking of risks; allocation of resources; projections of risk activities and risk priorities; and review of risk management systems.

41. Harvard Business School has identified six components of the business model which it believes may be relevant in the context of a turbulent and competitive business environment: value proposition; market segment; value chain structure; competitive strategy; revenue streams; and cost structure. See Chesbrough and Rosenbloom (2002).

42. In particular, catastrophic risks have three prominent characteristics loss distributions: fat tails, micro-correlations and tail dependence. With fat-tailed loss distributions, the probability of ever larger damages decreases more slowly than for thin-tailed distributions to which we are accustomed. Micro-correlations are small, positive, average correlations between risks that can have a large impact if such risks are aggregated. Tail dependence refers to the tendency of extreme losses to occur together. These three characteristics of catastrophic risks all combine to create, with low probability, the potential for enormous losses. See Kousky and Cooke (2012).

43. "The 2013 smoky haze marks the 10th occurrence of trans-boundary haze since the 1970s. For 2013, Singapore has claimed to suffer from economic losses estimated at USD 1 billion a week." *The Jakarta Post* (2013).

44. See Marsh Risk Consulting (2013).

45. Such as the industry the company is in, whether the company is operating predominantly in Singapore or has significant overseas operations, the mid- to long-term business strategies of the company.

46. See Principle 3.2 of the SGX (2011).

47. See OECD (2010).

48. The risk appetite is defined as "the amount of risk that an organisation is willing to seek or accept in the pursuit of its long term objectives". The definition of risk tolerance by Institute of Risk Management (IRM) is restated in the Guidance: "The boundaries of risk taking outside of which the organisation is not prepared to venture in the pursuit of its long term objectives."

49. See Rittenberg and Martens (2012).

50. Simone Heidema (2013) stated, "Risk appetite must be embedded into decision-making processes through specified risk tolerances and limits, and by controlling these processes".

51. See Pederson and Cheng (2012).

52. See Pederson and Cheng (2012).

53. See Singapore CFO Institute and PwC (2013).

54. See OECD (2011).

55. See FSB (2013).

56. The Code also sets forth the fundamental requirements with regard to an internal audit, including its effectiveness, independence and resource. The ACGC (2008) provides the details of the role and responsibilities of internal audit functions. Internal auditors are required to carry out its function according to the international standards which requires to evaluate the effectiveness and to contribute to the improvement of risk management processes. The Code 13.4 recommends that the Internal Auditor should carry out its function according to the standards set by nationally or internationally recognised professional bodies including the Standards for the Professional Practice of Internal Auditing set by The Institute of Internal Auditors. The Standards address the role of the internal audit activity in relation to the risk management (2120).

57. Citing a study by Singapore Management University, Mr David Gerald (Chairman of SIAS) noted that one-third of Singapore-listed companies do not have a full-time internal auditor. See *The Business Times* (2013).

58. The Securities Investors Association of Singapore (SIAS), Institute of Internal Auditors Singapore (IIAS) and Singapore Management University (SMU) called for mandatory internal audits. See *Straits Times* (2011).

59. See *The Business Times* (2013).

60. See ACRA (2010).

61. See ACRA (2010).

62. Ministry of Finance's Response to the Report of the Steering Committee for Review of the Companies Act. See the response to Recommendation 4.21. Available at: *www.acra.gov.sg/NR/rdonlyres/53C80533-E17B-4305-8DFB-B525419A131A/0/5NarrativeReportonCAAccountsandAudit.pdf*.

63. In the United States for example, an audit firm that "detects or otherwise becomes aware of a possible illegal act in the course of conducting an audit of an issuer (whether or not perceived to have a material effect on the financial statements of the issuer)" is required to ensure that the issuer has taken appropriate remedial measures and, under certain conditions, must report to the SEC (Section 10A of the Securities Exchange Act of 1934).

64. According to the survey by ACCA and SIAS (2011), almost all (94%) of respondents desired that the additional information be made available to the public at large and not be restricted to only the audit committee. This includes the relevant information regarding risk governance.

65. The OECD (2010) showed that these disclosures tend to be poor even though there appears to be economic returns to improved disclosure.

66. See OECD (2010).

67. See SGX (2011).

68. See Tijo (2009).

Bibliography

ACGC (2008), The Audit Committee Guidance Committee, "Guidebook for Audit Committees", October 2008, available at: *www.acra.gov.sg/NR/rdonlyres/49C641A3-1FF4-4E2D-99FC-71AC04E2C750/9909/Finalinsidetext241008cast.pdf*.

ACRA (2010), Accounting and Corporate Regulatory Authority (ACRA), "Guidance to Audit Committees on Evaluation of Quality of Work Performed by External Auditors", July, available at: *www.acra.gov.sg/NR/rdonlyres/1DC91E0E-2609-4BCB-946E-34609E2E80F5/16741/ACRASGXGuidancetoauditcommitteesv2.pdf*.

The Association of Chartered Certified Accountants (ACCA) and Securities Investors Association Singapore (SIAS) (2011), "The Value of Audit: Views from Retail (Private) Investors", July, available at: *www2.accaglobal.com/pdfs/international/singapore/VOAPAC*.

The Business Times (2013), "Listed Companies Must Have Internal Auditors", 5 September, originally available at: *www.businesstimes.com.sg/breaking-news/singapore/listed-companies-must-have-internal-auditors-sias-20130905*.

Chesbrough, H. and R.S. Rosenbloom (2002), "The Role of the Business Model in Capturing Value from Innovation: Evidence from Xerox Corporation's Technology Spin-Off Companies", *Oxford Journals – Industrial and Corporate Change*, Volume 11, Issue 3, available at: *http://icc.oxfordjournals.org/content/11/3/529.short*.

Choi, I. (2013), "When Do Companies Need a Board-Level Risk Management Committee?", International Finance Corporation Publication, available at: *www.ifc.org/wps/wcm/connect/444c0e804ef2b9df9e1bdf3eac88a2f8/PSO+31.pdf?MOD=AJPERES*.

Claessens, S., S. Djankov and L.H.P. Lang (2000), "The Separation of Ownership and Control in East Asian Corporations", *Journal of Financial Economics*, 58.

Committee of Sponsoring Organisations of the Treadway Commission (COSO) (2004), "Enterprise Risk Management – Integrated Framework", September, available at: *www.coso.org/documents/coso_erm_executivesummary.pdf*.

Ernst & Young (2012), *Board Matters Quarterly*, Issue 12, June, Singapore, *www.ey.com/SG/en/Services/Assurance/Board-Matters-Quarterly---Issue-12---June-2012---Editorial*.

FSB (2013), *Thematic Review on Risk Governance: Peer Review Report*, available at: *www.financialstabilityboard.org/publications/r_130212.pdf*.

FSB (2012), "Increasing the Intensity and Effectiveness of SIFI Supervision: Progress Report to the G20 Ministers and Governors", November 2012, available at: *www.financialstabilityBoard.org/publications/r_121031ab.pdf*.

Heidema, S. (2013), "How Singapore Financial Firms Must Utilise Risk Appetite", *Singapore Business Review*, 30 April, available at: *http://sbr.com.sg/financial-services/commentary/how-singapore-financial-firms-must-utilise-risk-appetite*.

The Jakarta Post (2013), "Governing the Risk of Haze and ASEAN Diplomacy", 28 June, available at: *www.thejakartapost.com/news/2013/06/28/governing-risk-haze-and-asean-diplomacy.html*.

Kay, J. (2012), *The Kay Review of UK Equity Markets and Long-Term Decision Making: Final Report*, July, available at: *www.ecgi.org/conferences/eu_actionplan2013/documents/kay_review_final_report.pdf*.

Kousky, C. and R. Cooke (2012), "Explaining the Failure to Insure Catastrophic Risks", *The Geneva Papers on Risk and Insurance*, 37.

KPMG (2010), "Charting a Safe and Sustainable Growth Journey: Singapore Enterprise Risk Management Survey 2010", available at: *https://www.kpmg.com/SG/en/IssuesAndInsights/ArticlesPublications/Documents/SgERMSurvey2010.pdf*.

KPMG and the Singapore Management University (SMU) (2009), "Oversight of Risk: The Role of Audit Committees Today", available at: *www.kpmg.com/SG/en/IssuesAndInsights/ACI-publications/Documents/ACI-OversightOfRiskRoleOfAuditCommitteesToday.pdf*.

Low, I. (2012), "The State of Corporate Governance Standards in Singapore", *The Directors' Bulletin*, Issue ???, Singapore Institute of directors, available at: *www.sid.org.sg/uploads/bulletin/documents/794_SID1233-5_2.pdf*.

Marsh Risk Consulting (2013), "Singapore Haze: Preparing for Business Continuity and Workforce Health and Safety", 24 June, available at: *http://asia.marsh.com/Portals/59/Documents/5327%20NCN%20Singapore%20Haze%20Prep%20for%20BCP.pdf*.

Monetary Authority of Singapore (MAS) (2010), "MAS Announces Composition of the Corporate Governance Councilation", 4 February, available at: *www.mas.gov.sg/news-and-publications/press-releases/2010/corporate-governance-council.aspx*.

OECD (2011), *Society at a Glance Asia/Pacific 2011*, Paris, available at: *www.oecd.org/els/soc/49263450.pdf*.

OECD (2010), *Corporate Governance and Financial Crisis: Conclusions and Emerging Good Practices to Enhance Implementation of the Principles*, Paris, available at: *www.oecd.org/daf/ca/corporategovernanceprinciples/44679170.pdf*.

Pederson, C. and Y.C. Cheng (2012), "Board Risk Governance: Effective Risk Oversight and Management Support", Oliver Wyman, available at: *www.oliverwyman.com/media/Board_Risk_Governance.pdf*.

Rittenberg, L. and F. Martens (2012), "Understanding and Communicating Risk Appetite", January, Research Commissioned by COSO (Committee of Sponsoring Organisations of the Treadway Commission), available at: *www.coso.org/documents/ERM-Understanding%20%20Communicating%20Risk%20Appetite-WEB_FINAL_r9.pdf*.

Singapore Exchange (SGX) (2013a), *Singapore Exchange Market Statistics Report*, July, available at: *www.sgx.com/wps/portal/sgxweb/home/marketinfo/market_statistics*.

Singapore Exchange (SGX) (2013b), "SGX-ST Listing Rules, Practice Note 12.2: Adequacy of Internal Controls", 2 April, *http://rulebook.sgx.com/net_file_store/new_rulebooks/m/a/MainBoard_April_2_2013.pdf*.

Singapore Exchange (SGX) (2011), "Guide to Sustainability Reporting for Listed Companies", available at: *http://rulebook.sgx.com/net_file_store/new_rulebooks/s/g/SGX_Sustainability_Reporting_Guide_and_Policy_Statement_2011.pdf*.

Singapore CFO Institute and PricewaterhouseCoopers LLP (2013), "State of Play: CFO & Enterprise Risk Management", May, available at: *http://cfoconnect.sg/sites/cfoconnect.sg/files/CFO-and-ERM-survey-report.pdf*.

Singapore Institute of directors (SID) and Singapore Exchange (SGX) (2010), *Singapore Board of directors Survey 2010*, available at: *www.sid.org.sg/web_surveys_awards/Board_survey*.

Singapore Law Reports (2007a), "PlanAssure PAC (formerly known as Patrick Lee PAC) vs. Gaelic Inns Pte Ltd. [2007] 4 SLR(R) 513; [2007] SGCA 41", *www.singaporelaw.sg/sglaw/laws-of-singapore/case-law/cases-in-articles/negligence/1607-planassure-pac-formerly-known-as-patrick-lee-pac-v-gaelic-inns-pte-ltd-2007-4-slr-r-513-2007-sgca-41*.

Singapore Law Reports (2007b), "JSI Shipping (S) Pte Ltd. vs. Teofoongwonglcloong (a firm) [2007] 4 SLR(R) 460; [2007] SGCA 40", *www.singaporelaw.sg/sglaw/laws-of-singapore/case-law/cases-in-articles/negligence/1606-jsi-shipping-s-pte-ltd-v-teofoongwonglcloong-a-firm-2007-4-slr-r-460-2007-sgca-40*.

Straits Times (2011), "3 Bodies Call for Mandatory Internal Audits", 11 October, available at: *www.iia.org.sg/downloads/ST%20-%20Pg%20B18%20-%20Oct%2011%20'11%20-%203%20bodies%20call%20for%20mandatory%20internal%20audits.pdf*.

Tan, L.H. (2006), "A Balanced Scorecard Approach to Survey Corporate Governance Practices in Singapore's Listed Companies: STI Companies and Government-Linked Companies" (1 May), available at SSRN: *http://ssrn.com/abstract=905048*.

Teen, M.Y. (2006), "Implementation and Enforcement of Rules in Singapore and the Case of China Aviation Oil", presented at the 2006 OECD Asian Roundtable, *www.oecd.org/daf/ca/corporategovernanceprinciples/37997933.ppt*.

Teen, M.Y. (2007), "Improving the Implementation of Corporate Governance Practices in Singapore", June, available at: *www.mas.gov.sg/~/media/MAS/Singapore%20Financial%20Centre/Why%20Singapore/Corporate%20Governance%20of%20Listed%20Companies/Publications/Full%20Report.ashx*.

Teik, L.C. (2009), "Dare to Challenge ! The SIAS Story", *Straits Times Press*.

Temasek (2013), Temasek Review 2013, available at: *www.temasekreview.com.sg*.

Tijo (2009), "Enforcing Corporate Disclosure", *Singapore Journal of Legal Studies*, 332-364, available at: *http://law.nus.edu.sg/sjls/articles/SJLS-Dec09-332.pdf*.

The World Bank (n.d.), "Market Capitalisation of Listed Companies (% of GDP)", *http://data.worldbank.org/indicator/CM.MKT.LCAP.GD.ZS*.

Yeo, G.H.H., P.M.S. Tan, K.W. Ho and S. Chen (2002), "Corporate Ownership Structure and the Informativeness of Earnings", *Journal of Business Finance & Accounting*, 29(7) & (8), Sept./Oct.

Yip, A. and J. Tan (2011), "Chapter 20: Singapore", *The Corporate Governance Review*, Law Business Research Ltd.

Chapter 4

Switzerland: The corporate governance framework and practices relating to risk management

This chapter, part of the sixth peer review based on the OECD Principles of Corporate Governance, *summarises the corporate governance framework and practices relating to corporate risk management in Switzerland, with a primary focus on large multinationals, but also covering state-owned enterprises (including at sub-federal level). The chapter was prepared by the OECD Secretariat (Winfrid Blaschke and Daniel Blume).*

4.1. Introduction

Switzerland has a large and diversified corporate sector, with many large multinationals having their headquarters in the country, as well as large numbers of strong and successful small and medium-sized enterprises (SMEs). This is reflected in the equity market capitalisation of the Swiss Exchange (SIX), which exceeded CHF 1 trillion (180% of GDP) at the end of 2012. Most of this is accounted for by the 20 largest stocks included in the SMI blue-chip index, and the rest by the SMI MID index comprising the 30 largest mid-cap stocks which are not included in SMI. It total, about 300 companies are listed on SIX, about 40 companies (all SMEs) are listed on the Berne eXchange, and the rest are unlisted.

The large Swiss companies are mostly widely-held, whereas in the small and medium-sized segment, companies almost always have a controlling owner. International investors are big shareholders in Swiss companies. Many international companies register their head offices, or those of their subsidiaries, in Switzerland. Outside the financial sector, the largest companies can be found in health care (Novartis, Roche), consumer goods (Nestlé, Richemont, Swatch), Industrials (ABB, Holcim, SGS), Basic Materials (Syngenta), Oil&Gas (Transocean), and Telecoms (Swisscom).[1]

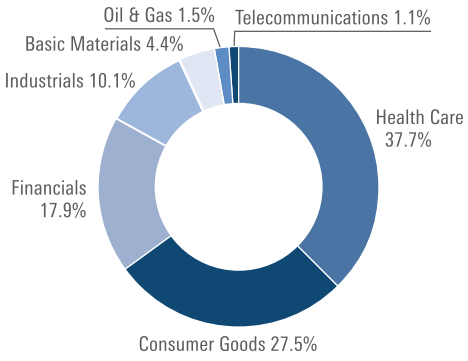
The Swiss federal government is the majority shareholder in one listed company (Swisscom, 56.8%), fully owns the Swiss Post, Swiss Railways, and RUAG (defence and aerospace), and also holds 99.7% of Skyguide (air traffic control). The ownership function is shared between the Federal Department of Finance (FDF) and the line ministries, i.e. the Federal Department of the Environment, Transport, Energy and Communications (DETEC), except for RUAG, where it is the Federal Department of Defence, Civil Protection and Sport (DDPS). At sub-federal level, the Swiss cantons are shareholders in a further 600 companies, mostly smaller ones. Some of them, however, are of significant size, notably cantonal banks and building insurers or energy suppliers held jointly by several cantons.

Given the importance of large Swiss companies, and the sectors they are involved in (e.g. energy, financial, pharmaceutical, telecoms, transport, all sectors where risk is inherent), it is perhaps not surprising that risk management has become an important issue for Swiss companies. Outside the financial sector, where UBS has drawn most attention since the financial crisis, the most prominent risk management failure has been Swissair,[2] but several of the other large Swiss corporates have also had to strengthen their governance following prominent risk management failures.

While Switzerland formally has a unitary board system, most of the larger companies essentially operate a dual board system, as boards of directors (BoD) can, but are not required to, delegate most of the day-to-day management of the company to an executive board. The BoD retains, however, the responsibility for a number of critical oversight tasks, defined in legislation, that cannot be delegated. Except at banks and insurers, the CEO is frequently a member of the board of directors, and may also serve as chairman of the board.[3] Staggered boards are common in Switzerland, but will be abolished with the introduction of mandatory one-year terms for board members (see Minder initiative in Box 4.1).

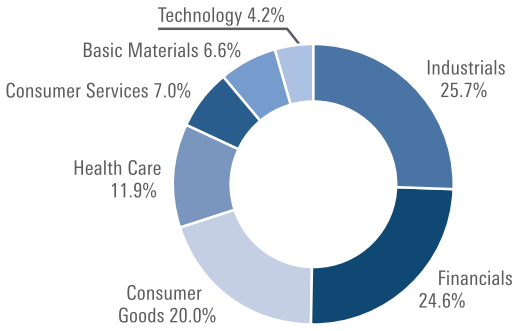
Figure 4.1. **Composition of Swiss equity indices (end-2013)**

SMI®



Health Care	**37.66%**
NOVARTIS N	19.29%
ROCHE GS	17.53%
ACTELION N	0.84%
Consumer Goods	**27.54%**
NESTLE N	21.08%
RICHEMONT	4.64%
SWATCH GROUP I	1.82%
Financials	**17.85%**
UBS N	6.09%
CS GROUP N	4.13%
ZURICH INSURANCE N	3.85%
SWISS RE N	2.82%
JULIUS BAER N	0.96%
Industrials	**10.05%**
ABB LTD N	5.44%
HOLCIM N	1.51%
SGS N	1.13%
GEBERIT N	1.02%
ADECCO N	0.95%
Basic Materials	**4.37%**
SYNGENTA N	3.31%
GIVAUDAN N	1.06%
Oil & Gas	**1.47%**
TRANSOCEAN N	1.47%
Telecommunications	**1.06%**
SWISSCOM N	1.06%
Total	**100.00%**

SMIM®



Industrials	**25.70%**
SIKA I	5.88%
KUEHNE+NAGEL INT N	5.66%
SCHINDLER PS	5.22%
SULZER N	2.92%
FISCHER N	2.11%
OC OERLIKON N	2.04%
DKSH N	1.87%
Financials	**24.58%**
BALOISE N	4.89%
SWISS LIFE HOLDING AG N	4.86%
PARTNERS GROUP N	3.83%
SWISS PRIME SITE N	3.60%
PSP N	2.62%
GAM N	2.44%
HELVETIA HOLDING N	2.33%
Consumer Goods	**19.99%**
ARYZTA N	5.41%
SWATCH GROUP N	4.63%
LINDT N	4.43%
LINDT PS	3.15%
BARRY CALLEBAUT N	2.36%
Health Care	**11.90%**
SONOVA N	5.40%
LONZA N	3.86%
NOBEL BIOCARE N	1.37%
STRAUMANN N	1.28%
Consumer services	**6.99%**
GALENICA N	3.75%
DUFRY N	3.24%
Basic Materials	**6.60%**
CLARIANT N	4.67%
EMS-CHEMIE N	1.94%
Technology	**4.24%**
LOGITECH N	1.58%
AMS	1.35%
TEMENOS N	1.31%
Total	**100.00%**

Source: SIX Swiss Exchange (2013), *www.six-swiss-exchange.com*.

Box 4.1. **Switzerland – The Minder Initiative (2013)**

In March 2013, the Swiss voting public approved the "Minder Initiative", which introduced significant changes to corporate governance rules in Swiss companies whose equity securities are listed on a Swiss (or foreign) stock exchange. The measure referred to as the Minder Initiative, named after Thomas Minder, a member of the Swiss Council of States and business executive, includes, among other features: a mandatory binding annual vote on the total remuneration for the board and executive management at the general meeting of shareholders, prohibits severance, advance, or transaction related pay for members of the board or executive management, and chair/board members that are individually elected by the shareholders on an annual basis. Any violation of the new rules would be subject to stiff sanctions, including imprisonment of up to three years and a fine of up to six times the annual compensation.

The text of the revised Art. 95 paragraph 3 of the Swiss constitution is as follows:[1]

In order to protect the economy, private property and shareholders and to ensure sustainable management of businesses, the law requires that Swiss public companies listed on stock exchanges in Switzerland or abroad observe the following principles:

(a) Each year, the Annual General Meeting votes the total remuneration (both monetary and in kind) of the board, the executive board and the advisory board. Each year, the AGM elects the president of the board or the chairman of the board and, one by one, the members of the board, the members of the Compensation Committee and the independent proxy voter or the independent representative. Pension funds vote in the interests of their policyholders and disclose how they voted. Shareholders may vote electronically at a distance; proxy voting by a member of the company or by a depositary is prohibited.

(b) Board members receive no compensation on departure, or any other compensation, or any compensation in advance, any premium for acquisitions or sales of companies and cannot act as consultants or work for another company in the group. The management of the company cannot be delegated to a legal entity.

(c) The company statutes stipulate the amount of annuities, loans and credits to board members, bonus and participation plans and the number of external mandates, as well as the duration of the employment contract of members of the management.

(d) Violation of the provisions set out in letters a to c above shall be sanctioned by imprisonment for up to three years and a fine of up to six years' remuneration.

The Swiss government approved, in November 2013, an ordinance implementing the constitutional amendment.[2] Its provisions come into force starting at the beginning of 2014. Shareholders would thus be able to vote on compensation for 2014 at the 2015 annual shareholder meetings. The ordinance will later be replaced by a federal law which will be approved by the Parliament.

1. Unofficial translation from *http://en.wikipedia.org/wiki/Swiss_referendum_%22against_rip-off_salaries%22*.
2. The implementing regulation is available (in German/French/Italian) at *www.ejpd.admin.ch/content/ejpd/de/home/dokumentation/mi/2013/2013-11-20.html*.

4.2. Risk management standards and codes

In terms of legislation, the *Swiss Code of Obligations (CO)* addresses risk management as one of the areas that the board of directors can delegate to the executive board, but must maintain oversight of.[4] In addition, a requirement that all companies must include information on the conduct of a risk assessment in the notes to the accounts was frequently interpreted as requiring companies to have a risk management system in place.

While this requirement was recently narrowed in terms of both coverage (now limited to larger companies) and effect (no longer part of the notes to the accounts), it has led many companies, including smaller ones, to pay more attention to risk management.[5]

The *Swiss Code of Best Practice for Corporate Governance (SCBP)*, issued by the business federation Economiesuisse in 2002 (revised in 2007), contains legally non-binding recommendations mainly to Swiss public limited companies with regard to internal controls and risk management. Non-listed economically significant companies are expected to be able to develop appropriate guidelines from the SCBP. The SCBP specifically recommends that the internal control system be geared to the size, complexity and risk profile of the company, and that it should, depending on the specific nature of the company, also cover risk management, with the latter covering both financial and operational risks.

Although there is no rule requiring mandatory conformity with a standard, Swiss listed companies use COSO's *Enterprise Risk Management Framework (COSO-ERM)*, the ISO 31000 *Guideline on Principles and Implementation of Risk management*, and/or the Austrian *ON-Regelwerk 49000 Risikomanagement für Organisationen und Systeme*. Several Swiss companies indicated that they closely follow the ISO 31000 Guideline.

With regard to all joint stock companies where the state is a partial or single owner, the Code of Obligations (CO) is applicable, in some cases (e.g. Swisscom) backed by additional provisions on public ownership in special law. According to their legal obligations (joint stock companies: Swiss Code of Obligations; statutory corporations: specific law based on Code of Obligations) as well as by the strategic objectives issued by the owner, all SOEs must run an adequate risk management system and report on their specific risk-assessment methods. For banks and insurers supervised by the Swiss Financial Market Supervisory Authority (FINMA), there are specific standards and guidance concerning risk management.[6]

Listed companies are subject to additional requirements (Stock Exchange Act, Directives by the stock exchange regulatory board), mostly regarding disclosure of their corporate governance practices, including those relating to risk management. According to the *SIX Swiss Exchange Directive on Information related to Corporate Governance*, listed companies have to publish in the annual report, based on the principle of "comply or explain", the structure of the BoD's information and control instruments *vis-à-vis* the issuer's executive committee, such as internal auditing, risk management systems, and management information systems.[7]

The following sections refer to rules or recommendations, where they exist, in the specific areas under review, and then describe actual practices in Swiss companies. While they only represent a snapshot of the situation in a limited number of (mostly large) listed companies, and may thus not necessarily representative of all Swiss companies, they do give a fair indication of the overall state of play of risk governance in the Swiss corporate sector.

4.3. The role of Swiss boards of directors

Legal requirements

The obligation of the BoD to oversee the company's enterprise-wide risk management follows from the legal definition of the specific inalienable responsibilities of the BoD, including the duty to oversee the executive management and to constitute an adequate organisation (CO art. 716a). Generally, Swiss law provides the board with significant organisational flexibility. But even with maximum delegation the board by law retains a list

of critical responsibilities that cannot be delegated and that significantly exceed those foreseen in foreign legal systems. The duty of care and loyalty (art. 717 CO) also includes the duty to be sufficiently informed to take company relevant decisions. This duty of information implies an assessment of the risks arising from business activity. Moreover, an effective and efficient risk management is required to conform to the demands of good corporate governance.[8]

According to the SCBP, the board of directors should provide for systems for internal control and risk management suitable for the company. It should take measures to ensure compliance with applicable rules and may also allocate compliance to the internal control system. The BoD should review at least once a year whether the principles applicable to themselves and the company are sufficiently known and constantly observed.

The members of the BoD and all persons engaged in the business management or liquidation of the company are liable both to the company and to the individual shareholders and creditors for any losses or damage arising from any intentional or negligent breach of their duties. A person who, as authorised, delegates the performance of a task to another governing officer is liable for any losses caused by such officer unless he can prove that he acted with all due diligence when selecting, instructing and supervising him (art. 754 CO).[9]

Board expertise

There are no explicit qualification requirements for general board members of Swiss (non-financial) companies. Indirectly, a minimum requirement with regard to knowledge about legal and economic issues may be derived from a ruling by the Federal Court with regard to liability claims of shareholders or creditors, whereupon the ignorance or incompetence of a member of the BoD does not constitute an exonerating circumstance. [10] Knowledge about legal and economic issues is expected to allow a member of the BoD to make a business judgment, and to enable him to recognise his limits and therefore seek advice.

Moreover, a requirement with regard to the independent participation in the overall governance of the company, to making his own judgment about the problems and solutions in the area of the organisation and finance and about the selection and the monitoring of the management may be derived from the fact that the execution of the board functions with regard to the non-transferable and irrevocable duties (CO art. 716a par. 1) is personal in nature. The SCBP recommends that a majority of members of the audit committee, including the Chairman, be financially literate. Some companies go further, requiring their audit committee chairs to be financial experts.

With respect to financial institutions, members of the BoD are expected to be fit and proper, i.e. suitable for the job. This includes having appropriate experience and expertise in areas relevant for the institution's business, including a sound understanding of the institutions major risks.[11]

Finding the right expertise for members of the BoD is sometimes mentioned as a problem in Swiss companies, more so in small and medium-sized companies than the large Swiss multinationals. It can also be difficult in SOEs, notably at the sub-federal level. Some cantons still send political nominees to represent their respective cantons in the boards of directors of SOEs jointly owned by several cantons.

Risk management in board meetings

Company practices regarding the discussion of risk management issues in board of directors meetings vary widely, depending largely upon the size of the company, the sectors in which it operates, the current economic and financial environment, and previous experience with risk management shortcomings. Most corporates (though not all SMEs) appear to hold an annual (or in some companies semi-annual), about 20-minutes discussion by the board of directors dedicated to risk management. These discussions draw on bottom-up and, in some cases, top-down, risk assessment performed within the company. Additional risk discussions are typically held in the context of the review of specific businesses or strategies, if warranted by relevant developments in the external environment, or in connection with major projects and mergers and acquisitions.[12]

The amount of detail that can be discussed in board risk assessments is of course limited, so some boards of directors focus primarily on signing off on an exhaustive list of risks (risk register), especially if there appear to be few changes from the previous years. Some advisors recommend, at a minimum, more frequent BoD discussions in sectors with significant risk exposures and/or at management level.[13] Problematic issues can be the perception that the risks have already been covered as part of strategy discussions (thus omitting risks unrelated to strategy), or as part of the company's internal control system (potentially missing risks not captured by internal controls). Observers note the importance of the board secretary in the preparation of the board discussion on risk management.

In terms of the risks that are reported to the board of directors, a common practice appears to be for management to report only a summary and those risks considered to be the top risks (e.g. "Top-10"). While this facilitates the board discussion, this pre-selection (CEO or CFO "filter") entails the risk that the top risks may not in fact be the most important risks needing board attention, e.g. because risks may have been selected using a faulty methodology or because management might not want to draw the attention of the board to them. Some companies therefore report the Top-50 risks rather than (or in addition to) the Top-10 to the board, even if the former may be discussed in less detail.

Board-level committees

The SCBP recommends that the audit committee or, as the case may be, the chairman of the board should get a report about internal control and risk management from the Internal Audit function. The audit committee should form an impression of the effectiveness of the internal audit and assess the quality of the internal control system, including risk management. Audit committees generally see it as their duty to evaluate the internal audit and the risk management.[14] The primary focus of audit committees naturally tends to be on financial risks, although there are some Swiss companies where the audit committee has a strong focus on non-financial risks such as technical compliance and IT risks.

In practice, risk policy is thus mostly prepared by management together with the audit committee and afterwards approved and at least once a year examined with regard to its appropriateness by the BoD.[15] In some of the large Swiss companies, the audit committee's involvement in risk mainly relates to process, while the substance of risks remains with other functions and committees, where applicable, reflecting a widely-held concern about splitting up ownership and oversight of the various risks. Companies with smaller boards are also less likely to set up additional board committees dealing with risk issues.

Board-level risk committees are becoming increasingly common in financial institutions. Depending on the size and complexity of the institution, FINMA normally expects a risk committee or a similar group at board of director level. A 2012 survey of corporate governance in Swiss companies found that among companies in the Swiss Market Index (SMI), all financial institutions had established a risk committee, but only 7% of non-financial institutions had done so (Deloitte, 2012). Not surprisingly, the share was found to be lower among the medium-sized companies included in the SMIM Index.

The only large listed (non-financial) company in Switzerland that has established a separate board-level risk committee is Novartis. Its five members, four of which are also members of the audit committee, normally meet four times per year for a minimum of two hours, and then debrief the full board. The risk committee explicitly has the right to invite the relevant "risk owner" to its meeting, thus setting up a direct reporting line.[16] One major advantage of this type of structure is seen in the fact that it permits the members of the risk committee get a deeper insight into strategic and operational risks, and to spend significantly more time on discussing risk management issues than is typically available in audit committee meetings.

In all the federally-owned SOEs, the board of directors have designated a board committee responsible for strategic risk governance. Most commonly, this task is assigned to the audit committee, except in the case of the Swiss Railways, where a specific risk committee has also been established to deal with non-financial risks.[17] While in the larger SOEs, and specifically joint stock companies, efforts to improve risk governance had already begun, Switzerland's 2006 reform of corporate governance policy has made the implementation of adequate risk management mandatory for all SOEs.

4.4. Risk management policies and structures in Swiss companies

Risk management policies

Risk management in Swiss companies is primarily seen as a responsibility of line management. Companies increasingly adopt risk policies that assign members of senior management as "risk owners" for particular risks. In larger companies, which have implemented extensive Enterprise Risk Management (ERM) systems, similar to those set up by financial institutions, the risks are typically reported from regional or facility-level on up (bottom-up approach) and then consolidated at group level, where they are sometimes filtered and/or complemented by additional risks (top-down approach).

While the implementation of bank-like risk management systems is often seen as contributing to companies taking a more systematic approach to risk management, their implementation in non-financial corporations faces significant challenges. The most important perhaps is the variety of risks that non-financial corporations face (including for example health, safety and environmental risks), risks that cannot easily be quantified, and even where that is theoretically possible, the company needs to keep such risks extremely low, often for ethical and reputational reasons. Risk management systems designed to deal primarily with financial risks are only of limited help in this context. Whereas some companies now use qualitative (non-financial) impact scales in their ERM processes, this does not appear to be a widespread practice.

Following the financial crisis, some Swiss companies have complemented their risk management with additional processes, such as stakeholder analysis, combination of top-down and bottom-up risk assessments, assets and liability management reviews, and holistic

approaches to governance, risk and compliance. Nevertheless, it appears that others (including some of the larger corporates) continue to rely heavily, within their risk management systems, on models that during the financial crisis have proved largely unsuitable even in the context of financial institutions. The probability assumptions going into so-called "heat maps", the standard instrument for summarising the company's risk situation, including for board discussions, can be questionable and lead to the underestimation of the likelihood of risk events, so that high-impact risks may not appear on the risk map, or, being in a "green corner" do not become the focus of management or BoD attention.[18]

Some companies have tried to address these issues by removing the probability assumptions from their systems, and/or by supplementing the standard models with scenario analyses. After several cases of risk management shortcomings that have caused significant reputational damage to Swiss companies, some companies have placed more emphasis on identifying (and mitigating) reputational risks, including where such risks can result from a lack of control over their suppliers and contractors spread out across various parts of the world.

Formalised risk appetite or tolerance statements can primarily be found in the financial sector. For financial institutions, FINMA expects the BoD to be involved in the setting of the overall risk policy and the risk appetite/risk tolerance of the institution. Such a process involves taking into account many factors, including company strategy, capital, liquidity, etc., as well as the various types of risks to which the institution is exposed and the company's internal mechanisms for managing and mitigating these. In some cases the extent of the risk to which the company is prepared to be exposed can be expressed quantitatively, in other cases semi-quantitatively or qualitatively.

In part due to the quantification problems referred to above, very few non-financial companies in Switzerland use a formal integrated risk appetite framework in the same way that financial institutions do. Many do, however, have "risk policies", issued by the board, that are intended to place limits on the taking of particular risks. Some companies have introduced sanctions for non-compliance with such policies and guidelines, notably in areas where non-compliance has in the past led to significant problems for the company.

One factor that may potentially affect risk appetite is of course remuneration.[19] Variable remuneration is much less widespread among Swiss corporates than among financial institutions, except at the highest management levels, where it can account for up to 80% of total compensation. Variable compensation in Swiss companies is increasingly paid in (blocked) shares rather than in the form of cash or options. It remains to be seen how remuneration systems in Swiss companies will change following the implementation of the "Minder initiative" that was approved by referendum in early 2013 and will come into force at the beginning of 2014 (see Box 4.1). It is possible that the binding say-on-pay rules, notably on variable compensation, and the ban on premiums for acquisitions or sales of companies may reduce management incentives to pursue certain high-risk business strategies.

Risk management structures

Many of the larger Swiss companies have established, at management level, one or more committees dealing with risk issues. These committees may either focus on particular risks, such as health, safety and environment (HSE), or discuss a wider array of risk within the same committee. Some companies have formed inter-disciplinary teams to

address risk, and in the largest companies, some of the committees may have various sub-committees, reflecting the global reach of their operations. Reporting tends to be to the Chief Financial Officer (CFO), almost always for financial risk, but often also for other risks. Some companies set up a separate committee for corporate governance and compliance risks, which then reports directly to the CEO or to an executive board member charged with corporate governance, corporate social responsibility, and/or compliance.

There is no recommendation or requirement in Swiss legislation or codes for non-financial companies to have a Chief Risk Officer (CRO).[20] A Deloitte (2012) survey found that almost 60% of SMI companies had established a Chief Risk Officer (CRO) or a Head of Group Risk Management. In 20% of the companies, the responsibility for risk management was supported by the Executive Committee, 15% by the Chief Executive Officer (CEO), and in a few companies the responsibility for risk rested with the Chief Financial Officer (CFO) (Deloitte, 2012).

The CRO, where it exists, is mostly positioned at the executive management level and reports either to the risk committee or the audit committee, but sometimes directly or additionally to the whole BoD. With regard to financial institutions, FINMA, in accordance with international standards, expects CROs to be independent, to have authority and no conflicts of interests. In non-financial companies, the title of CRO rarely exists, as responsibilities for risk are normally distributed among various members of the management team.

As a result, reporting lines for risk issues almost always go through the CFO (for financial risk) and/or the CEO (for other risks). A slightly modified approach is taken by corporates that, following major compliance problems, have established the position of Chief Compliance Officer (CCO). The CCOs then report directly (or through the internal audit function) to the audit committee.[21] Some companies have also established a "Head of Corporate Risk Management" function, covering both financial and non-financial risks, sometimes with a direct reporting line to the head of the board of directors' risk committee, where such a committee exists.

The SCBP recommends that companies should set up an Internal Audit function which should report to the audit committee or, as the case may be, to the chairman of the board. In practice, the large Swiss companies have established internal audit functions, but many small and medium-sized companies have not done so. Typically, consultants advise companies in Switzerland to set up internal audit functions when their number of employees exceeds either 1 000 or 2 000, but some significantly larger than that do not have internal audit functions.[22]

4.5. External assessments of the risk management framework

Disclosure practices

Since 2008, Swiss boards of directors (BoD) have had to include information on the conduct of a risk assessment in the notes to the accounts (art. 663b par. 12 CO). The risk assessment according to the (former) article 663b paragraph 12 of the CO is part of the company-wide risk assessment by which risks are monitored and controlled. At a minimum, the risks which have a material influence on the annual accounts had to be indicated. Factors to be considered include sector affiliation, company size, technological developments, labour market conditions, forms of funding, the liquidity position, the competition situation, the product mix, internal organisation, shareholder structure, the

external influence of interested third parties (stakeholders) and the environment.[23]

A new provision in the accounting law has replaced art. 663b CO and became effective 1 January 2013. This provision, which has to be implemented for the business year 2015, stipulates that only larger entities have to disclose information regarding the risk assessment.[24] This information will furthermore be included in the annual report ("Lagebericht") to the account, and no longer in the notes to the accounts (art. 961c par. 2 sub-sect. 2 CO). The expectation is that the new law will in particular alleviate the regulatory burden on smaller companies. The revised law itself does not further specify the disclosure requirements.

The Deloitte (2012) survey also covered the disclosure practices of Swiss companies regarding their risk management systems. The survey found that 45% of the companies in the SMI disclosed information about their risk policies in their annual reports or on their websites. Furthermore, little risk information was disclosed, the information disclosed was not concise, and only the most generic and inherent risks were disclosed. Many risk disclosures, even by some of the largest companies, indeed appear to be broadly worded, largely aimed to satisfy regulatory requirements and/or to serve as disclaimers to avoid legal liability. Risk disclosures tend to be somewhat more detailed in the context of security offering prospectuses and listings.[25]

External auditors

According to the Swiss Code of Obligations, the external auditor has to review the existence of an internal control system and take account of the internal system of control when carrying out the audit and determining the extent of the audit (CO art. 728a I/II). The statement in the notes to the accounts about the performance of the risk assessment required by the (former) article 663b paragraph 12 CO had to be reviewed by the external auditor. The information regarding the risk assessment in the annual report according to the new article 961c paragraph 2 subsection 2 CO ("Lagebericht") does not have to be reviewed by the external auditor.[26] The annual report must not however, contradict the economic position presented in the annual accounts (art. 961c para. 3 CO).

The external auditor issues to the BoD on an annual basis a comprehensive report, including statements pertinent to the internal control system, and the implementation and the result of the audit (art. 728b par. 1 CO).[27] Some of the large companies indicated that they also ask their external auditors to review their risk management system at least once or twice per year. For financial institutions, FINMA expects banks and insurers to periodically review the effectiveness of their risk management system, which includes periodic reviews by a third party such as the external auditor. In Switzerland, all persons engaged in auditing the annual and consolidated accounts, the company's establishment, a capital increase or a capital reduction are liable both to the company and to the individual shareholders and creditors for the losses arising from any intentional or negligent breach of their duties (art. 755 CO).

Investors and stakeholders

The perception among some of the widely-held Swiss companies is that most shareholders are not overly interested in how individual companies manage their risks, even if following the financial crisis some mainstream investors have started to take more interest in governance and risk management. This may in part be due to most shareholders holding widely diversified portfolios. The situation may also be somewhat

different in the case of companies with controlling owners, who typically have more of their personal wealth (and reputation) invested in the company. The main interest from the investor side, in terms of risk, appears to be whether the companies they invest in comply with environmental and social governance (ESG) criteria, in order to ascertain whether they qualify for inclusion in certain restricted fund portfolios. Rating agencies sometimes ask more questions, but those can also be geared primarily toward financial risk.[28] Proxy advisors regularly weigh in, however, on pay and incentive issues.

Externally, the main pressure for improving risk governance in Swiss companies has come from governments and regulators, such as in cases of problems with foreign anti-bribery and competition laws (or, mainly in the financial sector, tax and anti-money laundering legislation), or from the NGO side, notably in areas relating to health, safety and the environment. Whistleblowing by employees in order to draw attention to risks is still relatively rare in Swiss companies.[29]

The state as an owner

At federal level, any liability of the state as an owner for damages caused by the SOE's responsible organs, as well as any direct guarantee is explicitly excluded within the specific SOE law (where applicable). Explicit state guarantees for SOEs do exist, however, at cantonal level, notably for most of the cantonal banks. As risk management failures at SOEs can result in significant loss of taxpayer funds, either in terms of the equity invested in the SOE, or in the form of explicit or implicit guarantees ("too important to fail"), one would expect the state as an owner to insist that SOEs install sound risk governance structures.[30]

According the Swiss Federation's corporate governance guidelines, the Federation shall only exceptionally provide guarantees for SOEs, and in those cases impose strict risk policy provisions and systematically monitor, evaluate and disclose those risks.[31] In addition to the rules applying to listed companies (where applicable), the Swiss (federal) government's ownership function has essentially three channels to monitor and, in some cases, influence risk-taking in SOEs, namely through 1) the Federal Council's Strategic Objectives for the SOE, 2) regular ownership dialogues, and 3) the government's risk management system. At cantonal level, the number of policy tools may be more limited.[32]

Through the *Strategic Objectives*, the ownership function specifies, for a four-year-period, the main targets in business segments and topics including issues concerning risk (within the financial and personnel policy targets e.g. profitability, net debt limits, remuneration policy, general investment policy). In the case of Swisscom, for example, the federal government has prescribed compensation policies and imposed limits on M&A transactions through the Strategic Objectives, both explicitly and through the imposition of a leverage cap.[33]

Important activities and developments are expected to be raised and discussed in a *periodic dialogue* between the ownership function and the SOE representatives. This may include information on relevant changes in risk exposure. At federal level, these dialogues take place three to five times per year, usually on a quarterly basis (more frequently in the case of important transactions), and are normally attended by the director of the Swiss Federal Finance Administration, the relevant line minister, the chair of the board of directors, and the CEO.

As the ownership functions see their primary role as overseeing the board of directors in achieving their targets, rather than getting involved in (co-)governing the SOE, risk

management issues are mostly approached on a general level and not covered exhaustively. Ownership functions indeed appear cautious to delve too deeply into risk management issues, in order to avoid receiving confidential information not available to other investors, and/or to ensure that accountability remains with the company.[34]

Finally, the major risks emanating from (federal) state ownership are governed by the comprehensive *risk management system of the Confederation's central administration*. These risks, consisting of benefit losses, deterioration of assets or the obligation for refinancing the SOE in order to guarantee the fulfilment of public tasks, are regularly ascertained, evaluated and managed through this system. At sub-federal level, such systems are far less developed, as only some cantons have established comprehensive overviews of their participations and related risk exposures, and the quality of the risk analysis itself appears to vary significantly by canton.[35] The Swiss authorities consider that awareness of an active ownership policy grew substantially among politicians and administrations on sub-federal level in the past years and a dynamic process of professionalisation in these regards (including risk management policy) can be observed.

4.6. Conclusions

Following the financial crisis and a number of prominent risk management failures or shortcomings, Swiss companies have increased their attention to risk. While financial risk has thus been the focus of attention, the consequences of reputational risks are also becoming increasingly clear to companies. The strongest efforts to strengthen risk management can be observed at companies that have faced major risk issues in the recent past.

Outside of the financial sector, this increased attention is, however, not always reflected in a more formal approach to the organisation of risk management. Risk often remains the responsibility of business functions, with centralised risk management functions playing more of a coordinating and supportive role and reporting to management rather than to the board of directors. While a stronger emphasis on people rather than procedures has its advantages, the financial crisis has shown that risk is an area where formal procedures may also have a role to play.

Some corporates still heavily rely on models that were designed for the financial sector, and that have proven unreliable during the financial crisis. It would seem that boards would be well advised to place more emphasis on the identification, monitoring and mitigation of potentially catastrophic risks, regardless of their supposed (and sometimes underestimated) likelihood of occurrence.

In the case of state-owned enterprises, the state should ensure that, as part of the nomination process, the boards of directors have sufficient expertise to understand the risks incurred by the SOE. Without intervening in the day-to-day management of SOEs, the relevant ownership function should use all the opportunities it has, both in formulating strategic directives, and in its regular ownership dialogues, to ensure that the SOEs have proper risk management frameworks in place.

Notes

1. See Figure 4.1 for an overview of the largest Swiss companies, as reflected by the composition of the SMI (large-cap) and SMIM (mid-cap) stock exchange indices.
2. A lack of strategic risk management has widely been seen as an important factor in the collapse of Swissair in 2001.

3. In this case, the Swiss Code of Best Practice for Corporate Governance (margin No. 18) recommends the following: "*If, for reasons specific to the company or because the circumstances relating to availability of senior management makes it appropriate, the board of directors decides that a single individual should assume joint responsibility at the top of the company, it should provide for adequate control mechanisms. The board of directors may appoint an experienced non-executive member ("lead director") to perform this task. Such person should be entitled to convene on his own and chair meetings of the board when necessary.*"
4. Federal Act on the Amendment of the Swiss Civil Code (Part Five: The Code of Obligations) of 30 March 1911 (Status as of 1 January 2013), *www.admin.ch/ch/e/rs/220/index.html*.
5. Further revisions of Swiss corporate law are expected to be re-launched during 2014.
6. Among other places, these are found for banks in FINMA-Circular 08-24 and 08-21 (for operational risks) and for insurers in 08-32. The FINMA-Circulars may be downloaded at *www.finma.ch/e/regulierung/pages/rundschreiben.aspx* (only in German/French/Italian, some information also in English).
7. See *www.six-exchange-regulation.com/admission_manual/06_15-DCG_en.pdf*.
8. See Lehmann and Roth Pellanda (2009).
9. See also Gericke and Waller (2008).
10. Ref. BGE 97 II 411;122 III 200 (in French). Case law is limited in this area, however, as cases tend to settle, and those that become public mainly relate to delayed bankruptcy filings in the SME sector.
11. For the regulations applicable to the financial sector, see *www.finma.ch/e/regulierung/gesetze/Pages/default.aspx*.
12. In planned M&A transactions, some boards also hire external advisors to get additional independent advice.
13. Deloitte (2012) considers it good practice to conduct a risk assessment exercise on a yearly basis, with quarterly reviews as part of risk committee or management committee agendas. They further recommend that ERM reports be provided to the board on a quarterly basis, with relevant developments warranting ad-hoc reporting, and possibly risk assessments.
14. Ernst & Young, *The Audit Committee Impact on Swiss Companies*, 2005, p. 14, *www2.eycom.ch/publications/items/audit_committee_impact/en.pdf*; Audit Committees in *Der Schweiz – Verantwortung, Fähigkeiten und Arbeitsweisen, Bericht zur Studie* of Prof. Dr. Martin Hilb, Leiter des IFPM-HSG Center for Corporate Governance an der Universität St. Gallen, in Zusammenarbeit mit PricewaterhouseCoopers, 2005, p. 5, *www.pwc.ch/user_content/editor/files/publ_ass/pwc_audit_commitees*_ch_d.pdf (in German).
15. See Lehmann and Roth Pellanda (2009).
16. The charter of the Novartis Risk Committee can be found at *www.novartis.com/downloads/investors/corporate-governance/The_Risk_Committee.pdf*.
17. Furthermore, energy supplier Alpiq has established an "audit and risk committee".
18. While after the experience with the financial crises, companies seem to have largely moved away from the use of value-at-risk (VAR) models to capture the whole risk exposure of the company in one number, VAR models are still in use to capture financial risk.
19. See e.g. OECD (2011), "Board Practices: Incentives and Governing Risks", *Corporate Governance*, OECD Publishing, *dx.doi.org/10.1787/9789264113534-en*.
20. The nomination of a CRO is required in the financial sector.
21. See e.g. the Novartis Corporate Integrity Agreement with the US Department of Health and Human Services (*www.justice.gov/usao/pae/Pharma-Device/novartis_cia.pdf*), or Schindler's compliance programme (*www.schindler.com/com/internet/en/about-schindler/schindler-compliance-program.html*).
22. Banks and insurers are, however, required to have internal audit functions.
23. One example given are product defects. See *Message concernant la modification du code des obligations (obligation de révision dans le droit des sociétés) et la loi fédérale sur l'agrément et la surveillance des réviseurs du 23 juin 2004, pp. 3810/3811, www.admin.ch/ch/f/ff/2004/3745.pdf*. In German/Italian at *www.admin.ch/opc/search/?lang=de&language%5B%5D=de&product%5B%5D=fg&text=2003-2410*.
24. This includes all companies that must have their accounts reviewed by an auditor in an ordinary audit (art. 727 par. 1 CO): i) publicly traded companies and those that are required to prepare consolidated accounts; ii) companies that exceed two of the following thresholds in two successive

financial years: a) a balance sheet total of CHF 20 million; b) sales revenue of CHF 40 million; c) 250 full-time positions (annual average).

25. See e.g. Syngenta's Form 20-F filing with the US SEC (*www.syngenta.com/global/corporate/SiteCollection Documents/pdf/media-releases/en/2012-20-F.pdf*).
26. The government does, however, require SOEs (including non-listed ones) to have their "Lagebericht" audited. Under the draft regulations implementing the so-called "Minder Initiative" (see Box 4.1), external auditors would also have to review the compensation reports of listed companies.
27. For more information, see Böckli (2009).
28. After the financial crisis, Standard&Poor's, for example, started to include some commentary on companies' ERM programmes in its ratings reports.
29. In order to protect whistleblowers more effectively, the relevant legal provisions in the Code of Obligations are currently under revision. For more information on the revision until December 2012, see *www.bj.admin.ch/content/bj/fr/home/themen/wirtschaft/gesetzgebung/whistleblowing.html* (in German/French/Italian).
30. Notwithstanding the relevant provisions of sectoral regulators where applicable (e.g. FINMA for financial institutions).
31. *www.efv.admin.ch/f/downloads/finanzpolitik_grundlagen/cgov/CG_Leitsaetze_f.pdf* (in German/French/Italian).
32. Sectoral regulators, such as FINMA for financial institutions, can, however, oversee risk-taking at both federal and sub-federal level (e.g. cantonal banks).
33. See *www.uvek.admin.ch/themen/00681/00988/00992/index.html?lang=fr* (in German/French/Italian). See paragraphs 1.3 (requirement for appropriate risk management system), 2.4 (net debt capped at 2.1 times EBITDA), 3.4 (compensation), and 4. (M&A only if long-term value creation, manageable and taking due account of risks, explicit ban on buying foreign universal service suppliers).
34. In practice, it has, however, turned out to be difficult for the ownership function, at least at the political level, to deflect blame in cases of risk management problems in SOEs.
35. See Meister (2009).

Bibliography

Böckli, P. (2009), *Schweizer Aktienrecht*, *www.schulthess.com/buchshop/detail/ISBN-9783725558469*.

Boutellier, R., A. Fischer, M. Palazzesi and S. Buser (2006), *Ansatz zur Prüfung der Risikobeurteilung*.

Brühwiler, B. (2012), *Risikomanagement nach ISO 31000 und ONR 49000*, *https://shop.austrian-standards.at/search/Details.action?dokkey=481678*.

Deloitte (2012), *Corporate Governance – A spotlight on Swiss trends*, Second Edition, *www.deloitte.com/assets/Dcom-Switzerland/Local%20Assets/Documents/EN/Survey/Corporate%20Governance/2012/ch_en_Corporate_Governance_2012.pdf*.

Deloitte (2011), *Corporate Governance in Switzerland – A closer look at SMI companies*, *www.deloitte.com/assets/Dcom-Switzerland/Local%20Assets/Documents/EN/Tax/Legal%20Services/ch_en_Corporate_Governance_a_closer_look_at_SMI_companies.pdf*.

Economiesuisse (2007), *Swiss Code of Best Practice for Corporate Governance*, *www.economiesuisse.ch/de/PDF%20Download%20Files/pospap_swiss-code_corpgovern_20080221_en.pdf*.

Gericke, D. and S. Waller (2008), *Basler Kommentar zum Obligationenrecht II*, *www.schulthess.com/buchshop/detail/ISBN-9783719025250/Obligationenrecht-II.-Basler-Kommentar-zum-schweizerischen-Privatrecht*.

Hofstetter, K. (2002), *Corporate Governance in Switzerland*, *www.economiesuisse.ch/de/PDF%20Download%20Files/Studie_CorpLaw_20020701_e.pdf*.

Iseli, T. (2008), *Führungsorganisation im Aktien-, Banken- und Versicherungsrecht*, *www.schulthess.com/buchshop/detail/ISBN-9783725556076/Iseli-Thomas/F%C3%BChrungsorganisation-im-Aktien--Banken--und-Versicherungsrecht?bpmlang=fr*.

Kalia, V. and R. Müller (2006), Risk Management at Board Level, *www.haupt.ch/shop/oxid.php/sid/x/shp/oxbaseshop/cl/details/cnid/2e24821d128ecb191.96567415/anid/9783258072425/pgNr/7*.

KPMG and Universität Zürich (2004), *Interne Kontrolle in der Schweizer Praxis – Eine aktuelle Standortbestimmung*, *www.sgvw.ch/d/dossiers/Documents/dossier_22_kpmg_studie_d.pdf*.

Lehmann, A.P. and K.R. Pellanda (2009), *Agenda für ein (besseres) Risikomanagement durch den Verwaltungsrat*, *www.baerkarrer.ch/upload/publications/11_23_09LehmannRoth.pdf*.

Meister, U. (2009), *Kantone als Konzerne, Einblick in die kantonalen Unternehmensbeteiligungen und deren Steuerung*, *www.sgvw.ch/d/dossiers/Documents/dossier_28_referat_meister.pdf*.

Meister, U. and I. Scherrer (2012), *Kantone als Konzerne, Herausforderung Risikomanagement*, *www.dievolkswirtschaft.ch/de/editions/201206/pdf/Meister.pdf*.

Pfiffner, D.C. (2008), *Revisionsstelle und Corporate Governance*, *www.schulthess.com/verlag/detail/ISBN-9783037511329/Pfiffner-Daniel-Christian/Revisionsstelle-und-Corporate-Governance?bpmlang=fr*.

SIX Swiss Exchange (n.d.), *www.six-swiss-exchange.com*.

Swiss Federation (2009), *Strategische Ziele des Bundes für seine Beteiligung an der Swisscom AG 2010-2013*, *www.uvek.admin.ch/themen/00681/00988/00992*.

Treuhand-Kammer (2006), *Änderungen Obligationenrecht – Berücksichtigung des internen Kontrollystems in der Abschlussprüfung*.

Wyss, L. (2007), *Das IKS und die Bedeutung des (Legal) Risk Management für VR und Geschäftsleitung im Lichte der Aktienrechtsreform 2007*.

ANNEX A

Financial Stability Board: Sound risk governance practices

[Chapter V from FSB (2013), *Thematic Review on Risk Governance*]

Sound risk governance practices

Drawing from the findings of the review, including discussions with industry organisations as well as risk committee directors and CROs of several firms that participated in the review, the report sets out a list of sound risk governance practices. The list extracts some of the better practices exemplified by national authorities and firms. The sound practices also build on some of the principles and recommendations published by other organisations and standard setters, drawing together those that are relevant for risk governance. This integrated and coherent list of sound practices aims to help national authorities and firms continue to improve their risk governance.

The board of directors

1. The board:

a) avoids conflicts of interest arising from the concentration of power at the board (e.g., by having separate persons as board chairman and CEO or having a lead independent director where the board chairman and CEO are the same person);

b) comprises members who collectively bring a balance of expertise (e.g., risk management and financial industry expertise), skills, experience and perspectives;

c) comprises largely independent directors and there is a clear definition of independence that distinguishes between independent directors and non-executive directors;

d) sets out clear terms of references for itself and its sub-committees (including tenure limits for committee members and the chairs), and establishes a regular and transparent communication mechanism to ensure continuous and robust dialogue and information sharing between the board and its sub-committees;

e) conducts periodic reviews of performance of the board and its sub-committees (by the board nomination or governance committee, the board themselves, or an external party); this includes reviewing, at a minimum annually, the qualifications of directors and their collective skills (including financial and risk expertise), their time commitment and capacity to review information and understand the firm's business model, and the specialised training required to identify desired skills for the board or for director recruitment or renewal;

f) sets the tone from the top, and seeks to effectively inculcate an appropriate risk culture throughout the firm;

g) is responsible for overseeing management's effective implementation of a firm-wide risk management framework and policies within the firm;

h) approves the risk appetite framework and ensures it is directly linked to the business strategy, capital plan, financial plan and compensation;

i) has access to any information requested and receives information from its committees at least quarterly;

j) meets with national authorities, at least quarterly, either individually or as a group.

2. The risk committee:

a) is required to be a stand-alone committee, distinct from the audit committee;

b) has a chair who is an independent director and avoids "dual-hatting" with the chair of the board, or any other committee;

c) includes members who are independent;

d) includes members who have experience with regard to risk management issues and practices;

e) discusses all risk strategies on both an aggregated basis and by type of risk;

f) is required to review and approve the firm's risk policies at least annually;

g) oversees that management has in place processes to ensure the firm's adherence to the approved risk policies.

3. The audit committee:

a) is required to be a stand-alone committee, distinct from the risk committee;

b) has a chair who is an independent director and avoids "dual-hatting" with the chair of the board, or any other committee;

c) includes members who are independent;

d) includes members who have experience with regard to audit practices and financial literacy at a financial institution;

e) reviews the audits of internal controls over the risk governance framework established by management to confirm that they operate as intended;

f) reviews the third party opinion of the design and effectiveness of the overall risk governance framework on an annual basis.

The risk management function

4. The CRO

a) has the organisational stature, skill set, authority, and character needed to oversee and monitor the firm's risk management and related processes and to ensure that key management and board constituents are apprised of the firm's risk profile and relevant risk issues on a timely and regular basis; the CRO should have a direct reporting line to the CEO and a distinct role from other executive functions and business line responsibilities as well as a direct reporting line to the board and/or risk committee;

b) meets periodically with the board and risk committee without executive directors or management present;

c) is appointed and dismissed with input or approval from the risk committee or the board and such appointments and dismissals are disclosed publicly;

d) is independent of business lines and has the appropriate stature in the firm as his/her performance, compensation and budget is reviewed and approved by the risk committee;

e) is responsible for ensuring that the risk management function is adequately resourced, taking into account the complexity and risks of the firm as well as its RAF and strategic business plans;

f) is actively involved in key decision-making processes from a risk perspective (e.g., the review of the business strategy/strategic planning, new product approvals, stress testing, recovery and resolution planning, mergers and acquisitions, funding and liquidity management planning) and can challenge management's decisions and recommendations;

g) is involved in the setting of risk-related performance indicators for business units;

h) meets, at a minimum quarterly, with the firm's supervisor to discuss the scope and coverage of the work of the risk management function.

5. *The risk management function:*

a) is independent of business lines (i.e., is not involved in revenue generation) and reports to the CRO;

b) has authority to influence decisions that affect the firm's risk exposures;

c) is responsible for establishing and periodically reviewing the enterprise risk governance framework which incorporates the risk appetite framework (RAF), risk appetite statement (RAS) and risk limits.

   i) The RAF incorporates an RAS that is forward-looking as well as information on the types of risks that the firm is willing or not willing to undertake and under what circumstances. It contains an outline of the roles and responsibilities of the parties involved, the risk limits established to ensure that the framework is adhered to, and the escalation process where breaches occur.

   ii) The RAS is linked to the firm's strategic, capital, and financial plans and includes both qualitative and quantitative measures that can be aggregated and disaggregated such as measures of loss or negative events (e.g., earnings, capital, liquidity) that the board and senior management are willing to accept in normal and stressed scenarios.

   iii) Risk limits are linked to the firm's RAS and allocated by risk types, business units, business lines or product level. Risk limits are used by management to control the risk profile and linked to compensation programmes and assessment.

d) has access to relevant affiliates, subsidiaries, and concise and complete risk information on a consolidated basis; risk-bearing affiliates and subsidiaries are captured by the firm-wide risk management system and are a part of the overall risk governance framework;

e) provides risk information to the board and senior management that is accurate and reliable and periodically reviewed by a third party (internal audit) to ensure completeness and integrity;

f) conducts stress tests (including reverse stress tests) periodically and by demand. Stress test programs and results (group-wide stress tests, risk categories and stress test metrics) are adequately reviewed and updated to the board or risk committee. Where stress limits are breached or unexpected losses are incurred, proposed management actions are discussed at the board or risk committee. Results of stress tests are incorporated in the review of budgets, RAF and ICAAP processes, and in the establishment of contingency plans against stressed conditions.

Independent assessment of the risk governance framework

6. The board requires a periodic independent assessment of the firm's overall risk governance framework and provides direct oversight to the process.

7. The board or audit committee fully support the CAE and internal audit function by ensuring the CAE:

a) is organisationally independent from business lines and support functions and has unfettered access to the audit committee;

b) meets regularly with audit committee members outside of management's presence;

c) is appointed and dismissed with the approval of the audit committee (or chair of that committee);

d) has his/her performance, compensation, and budget reviewed and approved by the audit committee;

e) has the organisational stature, talent, and character needed to provide a reliable independent assessment of the firm's risk governance framework and internal controls and not be unduly influenced by the CEO and other members of management;

f) has the resources (people and systems) needed to effectively carry out the responsibilities of internal audit;

g) provides regular reports to the board or audit committee which summarise the results of internal audit's work, including overall conclusions or ratings, key findings, material risk/issues, and follow-up of management's resolution or identified issues.

8. The audit committee and risk committee periodically meet to ensure effective exchange of information, to ensure effective coverage of all risks include emerging risk issues relative to the RAF and business plans.

9. Internal audit meets its obligations to the board and supervisors by:

a) reporting audit findings, significant issues, and the status of remedial action directly to the board or audit committee on a regular basis;

b) providing an overall opinion of the design and effectiveness of the risk governance framework to the audit committee on an annual basis;

c) providing qualitative assessments of risks and controls as opposed to evaluating compliance with policies and procedures;

d) assessing whether business and risk management units are operating according to the RAF;

e) providing feedback on how the firm's risk governance framework and RAF compare to industry guidance and better practices as a means of influencing their evolution;

f) providing input to risk assessments and feedback on internal controls during the design and implementation processes;

g) escalating issues and concerns identified in the course of audit work or through internal whistle-blowing, complaint, or other processes and situations where appropriate remedial action is not being implemented in a timely manner;

h) being aware of industry trends and best practices;

i) meets, at least quarterly, with the supervisor.

10. Third parties

a) supplement (but do not replace) internal audit staff to increase coverage;

b) complement internal audit's skill sets with deeper expertise in select areas and/or broader context of industry practices;

c) are effectively supervised by the board or internal audit function to ensure accountability remains within the firm.

Source: Financial Stability Board (2013).

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where governments work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

The OECD member countries are: Australia, Austria, Belgium, Canada, Chile, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The European Union takes part in the work of the OECD.

OECD Publishing disseminates widely the results of the Organisation's statistics gathering and research on economic, social and environmental issues, as well as the conventions, guidelines and standards agreed by its members.

OECD PUBLISHING, 2, rue André-Pascal, 75775 PARIS CEDEX 16
(26 2014 01 1 P) ISBN 978-92-64-20862-9 2014

Corporate Governance

Risk Management and Corporate Governance

Contents

Consult this publication on line at ***http://dx.doi.org/10.1787/9789264208636-en.***

This work is published on the OECD iLibrary, which gathers all OECD books, periodicals and statistical databases.
Visit ***www.oecd-ilibrary.org*** for more information.

OECD*publishing*
www.oecd.org/publishing

ISBN 978-92-64-20862-9
26 2014 01 1 P