European Corporate Governance Institute (ECGI)
Law Working Paper No. 160/2010

~ and ~

Tilburg Law School Legal Studies
Research Paper No. 013/2010

June 10, 2010

The Risks of Corporate Legal Principles of Risk Management

Christoph Van der Elst
Tilburg University – Tilburg Law and Economics Center
Ghent University – Department of Business Law

ecgi

The Risks of Corporate Legal Principles of Risk Management

Law Working Paper N°.160/2010
June 2010

Christoph Van der Elst
Tilburg University, Ghent University and ECGI

ECGI Working Paper Series in Law

The Risks of Corporate Legal Principles of Risk Management

Working Paper N°.160/2010

June 2010

Christoph Van der Elst

Abstract

Corporate governance codes and corporate law contain provisions of internal control and risk management. First, this paper analyses the state of the art of these provisions in five Western European countries. The regulatory framework stretches from a Frühwarnsystem in Germany over the internal control report of the French chairman of the board and the internal control statement of the Dutch board to the European corporate governance statement and the UK sound risk management maintenance principle. Next, the paper provides insights how a sample of REIT's put the internal control and risk management rules and principles into corporate practice over the last decade. The analysis demonstrates that risk identification, financial risk management and risk response grew to an advanced stage while risk assessment - in particular the impact assessment of non-financial risks - and control activities are still in a development stage. The evidence shows that risk management practices are driven by regulation and legislation. Many but not all internal control features have been harmonized. The last section discusses some of the legal consequences of the finding that in view of both the regulatory developments and corporate practices new risks have emerged. First, the legal requirements as well as the eagerness of companies to fully comply with all best practices create a field of tension between the basic assumption of risk management frameworks in providing (only) reasonable assurance and the (reported) state of the art of managing and apparently controlling all (material) risks. Second, there is the risk related to the friction between the progress in identifying the risk management responsibilities of the concerned corporate parties while there is a standstill of other areas of law and in particular of the liability regimes.

Keywords: risk management, internal control, corporate governance, corporate law, internal control, corporate practices, corporate reporting

JEL Classifications: G32, K22, G30, M40

Christoph Van der Elst
Tilburg University, Ghent University and ECGI
University of Tilburg
Warandelaan 2
PO Box 90153
5000-LE Tilburg
The Netherlands
phone: 00-31-13-466.26.72, fax: 00-31-13-466.21.82
e-mail: C.vdrelst@uvt.nl

The Risks of Corporate Legal Principles of Risk Management

Christoph Van der Elst[1]
Tilburg University, Ghent University and ECGI

This paper is written at the moment the Icelandic Eyjafjallajokull volcano erupted. For almost one week the volcanic ash clouds caused most flights in Western and Northern Europe to be cancelled. Airlines had to spend millions to rearrange transport, accommodation and reimburse other costs of all stranded passengers, notwithstanding the *force majeure* situation. Force majeure can be defined as an event beyond the control of the parties to a contract which prevent, delay or hinder their ability to perform the contract. In many *force majeure* cases parties are excused from the performance of the contract (in whole or in part), or are entitled to suspend or defer performance of the contract. At first sight European airlines could invoke *force majeure* to justify the cancellation or delays in transport. However Regulation 261/2004 of the European Parliament and of the Council[2] protects passengers of airlines. The passengers have a right to compensation, to reimbursement and to care including meals, hotel and transportation to a hotel, and so on. In light of this passenger friendly regulation, European airlines face the huge risk of suffering from a financial catastrophe in case they have to cancel flights such as the volcano eruption caused them to do. Evidently, airlines must identify this type or risk, assess the risk and take appropriate actions like insure the risk or accept the risk. In the period to come we will see whether airlines did effectively *manage* this volcano risk. Risk management must be embedded in companies' organizations and the corporate constituents like the board of directors, risk management officers, audit committees and all involved employees, or in other words in corporate governance. The eruption did have an advantage too. According to some reports the flight bans caused emission drops of estimated 2.8m tonnes of CO^2, a short health cure for the planet. From that perspective, the cancellation was certainly environmental friendly behaviour.

The volcano eruption did not put risk management high on the agenda of lawmakers, policymakers, supervisory bodies, academics, corporate advisors or corporate constituents. Risk management was already acknowledged long before, not the least because of the recent financial crisis, the terrorist attack on the World Trade twin towers and the collapse of Enron, Worldcom, and other companies. However, together with the oil spill in the Gulf of Mexico, the alleged Goldman Sachs' fraudulent structuring and marketing of a synthetic mortgage bond, the (continuation of) skyrocketing bonus schemes, Greece's flirting with bankruptcy the volcanic gas cloud prevents any dwindling interest for risk management.

Before, risk management was considered as a typical management activity for which most social sciences, and in particular corporate law, hardly had any interest. The aforementioned events and incidents changed the awareness. Risk management and internal control became a

[1] I am grateful for the assistance and cooperation of Marijn van Daelen for section 3.
[2] Regulation (EC) No 261/2004 of the European Parliament and of the Council of 11 February 2004 establishing common rules on compensation and assistance to passengers in the event of denied boarding and of cancellation or long delay of flights, and repealing Regulation (EEC) No 295/91 (Text with EEA relevance) - Commission Statement, OJ L 46 of 17 February 2004, p. 1.

major concern in corporate law and corporate governance. A number of reforms introduced regulatory requirements regarding risk management. In general risk management is similar or even identical in different countries[3] in regards to the operations, the finance and the strategy of companies. Hence, it can be expected that the regulatory requirements are similar regarding the aforementioned topics. The compliance framework should differ more due to the other differences of the regulatory frameworks.

In the next sections risk management and the development of risk management in corporate governance will be addressed. Section 1 starts with the identification of risk management frameworks. Section 2 discusses the early requirements of corporate constituents and in particular the board of directors vis-à-vis risk management. Section 3 compares the new corporate law and corporate governance requirements in five Western European countries for appropriate internal control and risk management systems. Section 4 reports the development of risk management reporting of the real estate investment industry over the last decade. It illustrates both the significant increase of the role and importance of risk management and the difficult process to balance entrepreneurship and risk management. Section 5 concludes with a discussion of the state of the art on internal control and risk management. Our research object is the regulatory framework for the general industrial and commercial companies listed on a regulated stock exchange market. This review will not analyse the specific governance and risk management rulebooks of the financial, pharmaceutical, food, defence or other industry for which many specific and detailed (operational) risk management constraints are in operation nor will it investigate the particular requirements to mitigate fraud.

1. Holistic Risk Management Frameworks and Responsible Behaviour

The leading framework of internal control and enterprise risk management is provided in the COSO I and COSO II Reports.[4] This study therefore adopts the definition of internal control and enterprise risk management that is given in the 1992 and the 2004 reports:[5]

> Internal control is broadly defined as a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:
>
> - Effectiveness and efficiency of operations.
> - Reliability of financial reporting
> - Compliance with applicable laws and regulations

[3] But, of course, not in different industries or other differences between companies.
[4] M.M.A. van Daelen and A.C.N. van de Ven, 'Introducing risk management', in M.M.A. van Daelen and C.F. Van der Elst eds., *Risk management and corporate governance: interconnections in law, accounting and tax* (Cheltenham: Edward Elgar Publishing), forthcoming 2010, p. 6.
[5] Committee of Sponsoring Organizations of the Treadway Commission (COSO), Internal Control – Integrated Framework, Executive Summary (New York: AICPA Inc.) 1992, p. 2. (COSO I Report); Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Enterprise Risk Management – Integrated Framework*, Executive Summary (New York: AICPA Inc.) 2004, p. 2. (COSO II Report).

And

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

For a long period of time corporate risk management was closely related to financial management and the use of specific financial instruments like options, hedging swaps, and so on. 'In the jargon of finance specialists, the fundamental aim of corporate risk management can be viewed as the purchase of "well-out-of-the-money put options" that eliminate the downside while preserving as much of the upside as can be justified by the principle of comparative advantage',[6] the risk identification. Later, strategic, ethical and reputational evaluations and risk analyses were incorporated into more formal processes and were embedded in internal control and risk management assessments. This development was accompanied with the rise of the awareness and management of social, environmental and ethical influences of organisational activities. In many organisational activities the pressure to insert these components is significant. It resulted in long lists of risks to be managed. Table 1 provides an at random selected list of different risk types.

The evolution was integrated in the different components of an internal control framework. The framework must provide in an appropriate tone in the organisation, identify, assess and manage the risks the organisation is confronted with while aiming to reach its objectives, control these activities, communicate and inform the members of the organisation and monitor the control processes. The assessment of risk contains of two interrelated elements. First the probability an event occurs must be estimated. Next, the impact of this event must be analysed. The results of the assessment allow the company to manage the risks. In view of the organisation's objectives, the risks can be accepted, eliminated, controlled or shared. Later this framework was further developed into a risk management framework.

A risk management framework should help companies in achieving their strategic, operations, reporting and compliance objectives.[7] The financial crisis stressed the importance of the strategic oversight role of the board of directors in this process. In its thought paper, *Effective Enterprise Risk Oversight: The Role of the Board of Directors* COSO requires the board of directors to play a critical role in "overseeing an enterprise-wide approach to risk management" which include the understanding of the risk philosophy and the concurrence with the entity's risk appetite, the inquiry of the effectiveness of the risk management system, the review of the portfolio of risks and regularly being informed of the risk response to key risk exposures.[8] The paper is accompanied with the paper *Strengthening Enterprise Risk*

[6] R. Stulz, 'Rethinking Risk Management', *Journal of Applied Corporate Finance*, 9 (Fall, 1996/3), p. 8.
[7] Ibid., p. 3.
[8] Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Effective Enterprise Risk Oversight: The Role of the Board of Directors*, (New York: AICPA Inc.) 2009, p. 2-3.

Management for Strategic Advantage[9]to provide senior management guidance how to assist the board of director's monitoring role. guidance how to assist the board of director's monitoring role.

Table 1: Types of risks

Business	**Financial**	**Compliance**
Wrong business strategy	Liquidity risk	Breach of listing rules
Competitive pressure on price/market share	Market risk	Breach of financial regulations
General economic problems	Going concern problems	Breach of Companies Act requirements
Regional economic problems	Overtrading	Litigation risk
Political risks	Credit risk	Breach of competition laws
Obsolescence of technology	Interest risk	VAT problems
Substitute products	Currency risk	Breach of other regulations and laws
Adverse government policy	High cost of capital	Tax penalties
Industry sector in decline	Treasury risk	Health and safety risks
Take-over target	Misuse of financial resources	Environmental problems
Inability to obtain further capital	Occurrence of types of fraud	
Bad acquistion	Misstatement risk	
Too slow to innovate	breakdown of accounting system	
	Unrecorded liabilities	
	Unreliable accounting records	
	Penetration and attack of IT systems	
	Decisions based on incomplete information	
	Too much data and not enough analysis	
	Unfulfilled promised to investors	

Operational and other	
Business processes not aligned	Quality problems
Failure of major change initiative	Lack of orders
Loss entrepreneurial spirit	Failure of major project
Stock-out of raw materials	Loss of key contracts
Skills shortage	IT inability
Physical disasters	Failure of outsource provider
Failure to exploit intangibles	Industrial action
Loss of intangible assets	Failure of technology project
Breach of confidentiality	Lack of employee motivation
Loss of physical assets	Lack of employee efficiency
Lack of business continuity	Inability to implement change
Succession problems	Ineffective processing of documents
Loss of key people	Poor brand management
Inability ro reduce cost base	Product liability
Tough contract obligations	Ineffective management process
Over-reliance	Exploiting employees overseas
Failure of new product/services	Other business probity issues
Poor service levels	Other reputional problems
Failure to satify customers	Missed business opportunities

Source: ICAEW, *Implementing Turnbull – A Boardroom Briefing* (London, 1999), p. 15. (minor adaptations)

[9] Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Strengthening Enterprise Risk Management for Strategic Advantage*, (New York: AICPA Inc.) 2009, p. 24.

Legislators and regulators used these risk management developments to require companies to install risk management systems and report on this. The next two sections briefly address the legislative processes both at the European level and in five European Member States. It provides the impetus to analyse the risk management systems that the business community is using.

2. Regulatory Risk Management and Internal Control

2.1. Early developments

Over the last decade risk management became more and more embedded in corporate law and corporate governance. The entrenchment followed the development of interpreting the duties of the board of directors and management of large (listed) companies. Different steps in this development can be identified.

In older editions of companies' acts it was generally stated that 'the business of the company shall be managed by the directors who may exercise all the powers of the company'.[10] According to the Dutch, Belgian and French Code it was and still is the duty of the board of directors to govern the company[11], whilst the Germany the management board had to and must direct the companies and the supervisory board must supervise the management of the companies.[12] An article or section regarding the representation of the company follows this management duty.[13]

In some countries, like the Netherlands, the requirement to govern is further explained as the duty to properly manage and protect the assets of the company.[14] However, most acts remain silent or point at specific duties like the duty to prepare and provide timely (financial) information[15] and answer all questions with regard to the items on the agenda of the general meeting and the reports.[16] Any further clear legal guidelines as to what the board is required to do in order to meet this general duty of governing are lacking. Some corporate legal scholars fill the absence of legal directives. De Wulf analyses the Belgian implied obligations. The board of directors has a legal duty to assess the continuity of the company which requires a decent internal control system. The board of directors must adjust the valuation rules as soon as discontinuity is discovered.[17] The analysis shows that the internal control system must

[10] Regulation 70 of the U.K. Table A edition 1985. The Companies Act 1985 is imprecise and only imposes that the duty of the directors is owed to the company (section 309 (2) CA 1985).
[11] Book 2:129 Dutch Civil Code, Article 53 Belgian Companies Act 1935 and Article 89 French Companies Code 1966.
[12] Article 76 (1) and article 111 (1) German Stock Corporation Act 1965.
[13] Book 2:130 Dutch Civil Code, Article 54 Belgian Companies Act 1935; in France the chairman of the board of directors represented the company (article 113 French Companies Code 1966).
[14] Book 2: 9 Dutch Civil Code.
[15] Article 221, 226 and 233 Companies Act 1989, Book 2:141 Dutch Civil Code (to the supervisory board), and article 92 Belgian Companies Code and 341-1 French Companies Code 1966 (amended in 1984) (to the general meeting).
[16] See for example Article 540 Belgian Companies Code
[17] H. De Wulf, *Taak en loyauteitsplicht van het bestuur in de naamloze vennootschap* (Antwerpen: Intersentia, 2002), p. 282-284.

(only) provide reasonable assurance that the (internal and external) financial reporting is adequate but there are no requirements as to which framework must be used.

Since the last decade of the former millennium, corporate governance entered into the spotlight and remained there ever since. According to the Cadbury Code 'corporate governance is the system by which companies are directed and controlled' and 'boards of directors are responsible for the governance of their companies'.[18] The many corporate governance codes serve as a handle to flesh out a number of duties of the board of directors. These governance duties of the board of directors which were - at best - hidden in vague corporate sections or articles were put in the spotlight and clarified, first in a number of voluntary recommendations, later on in mandatory *comply or explain* rules and finally in compulsory legal obligations. Together with the development of corporate governance rules and frameworks, internal control and risk management requirements matured.

The Cadbury Committee argued that the legal duty to manage the company requires the board of directors to establish a 'system of internal control over the financial management of the company'.[19] The board must report 'on the effectiveness of their system of internal control and that the auditors should report thereon'.[20] It is the duty of the audit committee to review the statement on internal control systems. It was soon ascertained that companies experienced significant difficulty applying these recommendations. The 1994 Rutteman Report added the requirement of the board to report their responsibility regarding the internal control system, to provide a description of the procedures and an assessment of the effectiveness including a confirmation of this assessment and a statement that internal control only provides reasonable assurance.[21]

The Cadbury Code (and the Rutteman report) was a frontrunner. Similar first generation corporate governance reports on the continent were less developed as regards internal control and risk management requirements. In France, the first Vienot report of 1995 required the establishment of an audit committee which must verify the internal procedures for collecting information and checking its reliability.[22] The scope was clearly limited to the effectiveness of the system to provide reliable financial information. Two of the three Belgian corporate governance reports that were published in 1998 recommended that the board of directors 'ensures that an efficient internal control system is in place' and that 'executive management develops and implements the tools necessary to allow appropriate and effective internal

[18] Committee on the Financial Aspects of Corporate Governance, *The Financial Aspects of Corporate Governance* (London, December 2002), Recommendation 2.5.
[19] Committee on the Financial Aspects of Corporate Governance, *The Financial Aspects of Corporate Governance* (London, December 2002), Recommendation 4.31.
[20] Committee on the Financial Aspects of Corporate Governance, *The Financial Aspects of Corporate Governance* (London, December 2002), Recommendation 4.31-4.32.
[21] L. Spira and M. Page, 'Risk Management:The reinvention of internal control and the changing role of internal audit', *Accounting, Auditing & Accountability Journal*, 16 (1993), p. 649; B. Rayton and S. Cheng, *Corporate Governance in the United Kingdom: Changes to the Regulatory Template and Company Practice from 1998 to 2002*, University of Bath Working Paper (2004.13), p. 29-30.
[22] C.N.P.F.-A.F.E.P., *The Board of Directors of Listed Companies in France* (Paris,July 2005), p. 20.

control'.[23] The Dutch 1997 Peters report contained more detailed guidelines for both the management board and the supervisory board. According to recommendation 4.2. and 4.3. the management board was required to report to the supervisory board which risks strategy and policy entails and the results of the assessment of the internal control system for financial reporting. Simultaneously the board was required to establish effective systems for internal control. The supervisory board had to discuss at least once a year the 'risks of the company' as well as the results of the assessment of the management board of the systems of internal control.[24] In Germany, corporate governance codes were only developed after the first legislative changes regarding internal control systems were issued.

Overall, the corporate governance requirements regarding internal control and risk management were of a general nature and immature. First, only the Rutteman report defined internal control. As a consequence, internal control was often but not exclusively related to the internal or external financial reporting process, which is considered as one of the three – and later four – objectives of the broader risk management. Second, the process of achieving this objective was not identified. At best the internal control related guidelines identified some of the different duties to assure an appropriate internal control framework was in place which included the identification of risks, the effectiveness of *the system* and reporting to the shareholders or the supervisory board. Third, the recommendations contained hardly any clear guidance as to which corporate constituent is responsible for the different types of internal control objectives. In some governance codes duties were assigned to *owners* which were identifiable from a management perspective, but not from a legal perspective. Even nowadays the position of executive management is not always clarified. Fourth, notwithstanding many aspects of internal control and risk management are similar or even identical in different industries and countries, different bodies were responsible for similar duties. The Dutch management board, the British board of directors and the French audit committee are accountable for the assessment of the internal control system for financial reporting. Finally, some of the recommendations seem to conflict with each other. The Dutch management board must report on the evaluation of the internal control system for financial reporting but the supervisory board has to receive the assessments of all the different systems of internal control. Whilst some of the members of the different committees on corporate governance were familiar with the developments of the Committee of Sponsoring Organizations (COSO) the first generation of corporate governance codes clearly opted for a formal approach of best practices.

After the publication of the first generation of corporate governance codes but before the triggering events on the stock markets at the turn of the millennium, the German Parliament started with specific corporate legislative requirements regarding operational internal control

[23] Belgian Commission on Corporate Governance, *Recommendations of the Market Authority of the Brussels Stock Exchange* (Brussel, December 1998), recommendation 4.4; VBO/FEB, *Corporate Governance Recommendations* (Brussel, December 1998), recommendation 4.5. The third corporate governance report of the Belgian Banking and Finance Commission was limited to corporate governance information to be disclosed. This code contained no specific recommendations on internal control or risk management.

[24] Committee on Corporate Governance, *Recommendations of corporate governance in the Netherlands* (Amsterdam, June 1997), Recommendation 3.4.

in the German Control and Transparency in Business Act (KonTraG). According to the German Companies Act the management board has to establish an early risk recognition system. The system must provide assurance that material risks that can endanger the going concern of the company or, according to the German literature, can impair the net worth, financial position and results of the company in a sustainable matter[25], will be identified. The German law requires a system to be set up but only to the extent that risks that can cause material damage can be identified at an early stage. The management report must also report on the risks of the future development of the company. Moreover, auditors must control the risk early recognition system. The German Accounting Standards Board issued the German Accounting Standard nr. 5 assisting the German auditors in their control assessment of the management report. The Standard goes beyond the legal requirements and as a consequence the risk report provides information that exceeds the information that is acquired by the early recognition system.[26]

It is generally argued that KonTraG does not require the management board to establish a risk management system that covers all different areas. However the first German corporate governance code emphasizes that the management board must regularly inform the supervisory board 'about all relevant matters regarding business development, risk exposure and risk management of the company and major group subsidiaries' and immediately if the risk exposures 'change significantly against plan'.[27] The audit committee that should be established at the supervisory board level must address risk management.[28] German best practices broadened the legislative scope of KonTraG.

2.2. State of the Art of Internal Control and Risk Management in Corporate Law

The corporate scandals at both sides of the Atlantic drove politicians to new legal initiatives like the Sarbanes-Oxley Act, European Directives and many national European Member States initiatives. It coincided with the identification or at least recognition of board committees and types of directors. Next, corporate governance provided detailed recommendations as to how to implement internal control frameworks. The work of COSO is acknowledged or incorporated and further guidance is provided, like the UK Turnbull report or the French framework of the 'Groupe de travail "de place"'. The aim of most plans was to restore trust and ensure that companies have adequate controls to mitigate the identified risks. Some Parliaments issued new mandatory requirements regarding risk management and internal control, like the French NRE-Act and LSF-Act.[29] In Germany, the United Kingdom

[25] K. Schmidt and M. Lutter, *Aktiengesetz Kommentar* (Köln, O. Schmidt Verlag, 2008), p. 1035-1036.
[26] M. Dobler, *Auditing Corporate Risk Management – A Critical Analysis of a German Particularity* (LMU paper 2001-03, November 2003), p. 3.
[27] German Panel on Corporate Governance, *Corporate Governance Rules for Quoted German Companies* (2000) , p. 3-4.
[28] German Panel on Corporate Governance, *Corporate Governance Rules for Quoted German Companies* (2000), p. 11.
[29] Law nr. 2001-420 of 15 May 2001 relative aux nouvelles régulations économiques, *Official Gazette* nr. 113 of 16 May 2001, p. 7776; Law nr. 2003-706 of 1 August 2003 de sécurité financière, *Official Gazette* nr. 177 of 2 August 2003, p. 13220. The Breton Law of 2005 (Law nr. 2005-842 of 26 July 2005, *Offical Gazette* of 27 July

and the Netherlands a more balanced approach that combines features of mandatory requirements in combination with best practices were tuned to one another. Belgium opted only to transpose the European Directives and introduced a voluntary corporate governance code. Since 2010 this country adheres to the practices of its neighbouring countries. It transposed the European requirements to publish a corporate governance statement containing a description of the mean features of a risk management system for financial reporting and a mandatory comply or explain corporate governance regime.

These legislative and regulatory developments coincided and as a consequence convergence is not guaranteed, the exception of the European Corporate Governance Forum not considered. It does not come as a surprise that many companies face serious difficulties as to the scope and the content of the European and national requirements of internal control and risk management.

2.2.1. European Developments

At the European level the 2004 Transparency Directive requires that issuers' annual and interim reports include 'a description of the principal risks and uncertainties that [it] face[s]'.[30] The requirement to disclose the principal risks and uncertainties obliges companies to install at least a risk and uncertainty identification system. Similar requirements can be found in the Prospectus Directive 2003/71/EC and Commission Regulation 809/2004 that oblige companies to include risk factors in the prospectus.[31] The list of risk factors must comprise company-specific risks and/or risks related to the securities issued that are material for taking investment decisions.[32]

The 2006 amendment to the Fourth and Seventh company law directives requires an annual corporate governance statement from listed entities. This statement must contain 'a description of the main features of the company's internal control and risk management systems in relation to the financial reporting process'.[33] On the consolidated level, 'a

---

2005) has limited the scope of the internal control reporting requirements to French joint stock companies and the Law nr. 2008-649 of 3 juillet 2008 (*Official Gazette* nr. 155, 4 July 2008, p. 10705) portant diverses dispositions d'adaptation du droit des sociétés au droit communautaire further elaborated the requirements.

[30] Article 4, paragraph 2, subpart c and article 5, paragraph 4 Directive 2004/109/EG of the European Parliament and the Council of 15 December 2004 on the harmonisation of transparency requirements with regard to information about issuers whose securities are admitted to trading on a regulated market, OJ L 390, p. 38.

[31] For an analysis of the risk factor sections of prospectuses, see M. M. A. van Daelen, *Risk Management Solutions in Business Law: Prospectus Disclosure Requirements*, 21 October 2008. (Available at SSRN: http://ssrn.com/abstract=1287624.)

[32] Article 2 under (3), Commission Regulation (EC) No. 809/2004 of 29 April 2004 implementing Directive 2003/71/EC of the European Parliament and of the Council as regards information contained in prospectuses as well as the format, incorporation by reference and publication of such prospectuses and dissemination of advertisements, OJ L 149, p. 1.

[33] Article 1, paragraph 7, subpart c, Directive 2006/46/EC of 14 June 2006 of the European Parliament and of the Council amending Council Directives 78/660/EEC on the annual accounts of certain types of companies, 83/349/EEC on consolidated accounts, 86/635/EEC on the annual accounts and consolidated accounts of banks and other financial institutions and 91/674/EEC on the annual accounts and consolidated accounts of insurance undertakings, OJ L 224 of 16 August 2006, p. 1.

description of the main features of the group's internal control and risk management systems in relation to the process for preparing consolidated accounts' must be provided.[34] The statement can be integrated in the management report or be published as a separate report. There are some legal differences between the two publication methods but in both cases the auditor's opinion is required to cover the consistency of the main features of the company's internal control and risk management systems in relation to the financial reporting process. As a minimum, the auditor will have to control the availability in the corporate governance statement of the description of the main features of the system in relation to the financial reporting process and issue a consistency opinion. The Directive did not provide any guidance as to the level of work required nor did it oblige the auditor to start a forensic audit.[35]

The 2006 directive on statutory audits stipulates that public-interest entities must establish an audit committee (or alternative body) to monitor the financial reporting process and to monitor the effectiveness of the company's internal control, internal audit where applicable, and risk management systems.[36] According to recital 24 of this directive, an audit committee and an effective internal control system help to minimise financial, operational, and compliance risks, and enhance the quality of financial reporting. The statutory auditor must also 'report to the audit committee on key matters arising from the statutory audit, and in particular on material weaknesses in internal control in relation to the financial reporting process.'[37] In its Statement on Risk Management and Internal Control, the European Corporate Governance Forum confirmed that company boards are responsible for monitoring the effectiveness of internal control systems but pleaded against a legal obligation for boards to certify the effectiveness of internal controls.[38] The European Commission's recommendation on independent directors and committees of the board[39] recommends the audit committee to assist the board in its task to, e.g.:[40]

- review at least annually the internal control and risk management systems, with a view to ensuring that the main risks (including those related to compliance with existing legislation and regulations) are properly identified, managed and disclosed;
- ensure the effectiveness of the internal audit function, in particular by making recommendations on the selection, appointment, reappointment and removal of the head of the internal audit department and on the department's budget, and by monitoring the

[34] Article 2, paragraph 2, Directive 2006/46/EC.
[35] For an analysis of the new requirements, see FEE, *Discussion Paper for Auditor's Role Regarding Providing Assurance on Corporate Governance Statements* (Brussel, November 2009) p. 71.
[36] Article 41, paragraph 2, sub a and b, Directive 2006/43/EC of 17 May 2006 of the European Parliament and of the Council on statutory audits of annual accounts and consolidated accounts, amending Council Directives 78/660/EEC and 83/349/EEC and repealing Council Directive 84/253/EEC, OJ L 157 of 9 June 2006, p. 87.
[37] Article 41, paragraph 4, Directive 2006/43/EC.
[38] Paragraph 6, European Corporate Governance Forum, *Statement on Risk Management and Internal Control*, (Brussels, June 2006), p. 5. The full text of the statement is available at: http://ec.europa.eu/internal_market/company/ecgforum/index_en.htm.
[39] Commission Recommendation of 15 February 2005 on the role of non-executive or supervisory directors of listed companies and on the committees of the (supervisory) board, OJ L 52 of 25 February 2005, p. 51.
[40] Commission Recommendation, OJ L 52 of 25 February 2005, Annex I, Committees of the (supervisory) board, p. 61.

responsiveness of management to its findings and recommendations. If the company does not have an internal audit function, the need for one should be reviewed at least annually;
- review the effectiveness of the external audit process, and the responsiveness of management to the recommendations made in the external auditor's management letter.

Both the Audit Directive and this recommendation focus on the monitoring role of the audit committee, but they assign different roles to the audit committee with regard to monitoring the internal control system and its effectiveness, respectively. According to the Audit Directive, the committee has a duty to perform the overall monitoring of the financial reporting process but only has to monitor the effectiveness of the global system, whilst the recommendation stresses the committee's duty of monitoring the global internal control system but the committee only has to assess the effectiveness of the internal audit function and external audit process.[41]

2.2.2. The UK Approach

The UK immediately opted for a comply or explain corporate governance regime. The London Stock Exchange introduced a requirement into the Listing Rules that demanded companies to include a statement of (non-)compliance with the provisions of the report in their annual report and accounts.[42] This approach is more or less maintained but is thwarted by the mandatory European requirements. After an update of the remuneration guidelines in the 1995 Greenbury report, the Hampel Committee issued its report in January 1998.[43] This report emphasized that the board should maintain a sound system of internal control to safeguard shareholders' investment and the company's assets. The Hampel report furthered internal control by arguing that this system not only covers financial controls but also operational and compliance controls, as well as risk management.[44] Following the recommendations of the Hampel Committee, the London Stock Exchange issued the Combined Code on Corporate Governance in June 1998. In the UK the Institute of Chartered Accountants of England and Wales provided further guidance regarding internal control and risk management via the Turnbull report in 1999. The Turnbull Committee was set up in September 1998 to provide guidance on how to apply this 1998 Combined Code, especially the internal control provision. The report sets out best practices on internal control and assists listed companies in applying the aforementioned principle and its associated provisions of the Combined Code.

---

[41] The latter duty being further limited to specific subtasks, namely the responsiveness of the management and the functioning of the head of internal audit.

[42] See also Cadbury Committee, *Report on the Financial Aspect of Corporate Governance* (London: Gee, 1992) (Cadbury Report)) , Section 1.3.

[43] The Hampel Committee was established in November 1995 on the initiative of the Chairman of the Financial Reporting Council (Sir Sydney Lipworth).

[44] Hampel Committee, *Committee on Corporate Governance – Final report* (London: Gee, 1998) (Hampel Report)), Section D (Accountability and Audit) under II and subsection 2.20, p. 21.

The board of directors is responsible for maintaining a sound system of internal control and must ensure that the system is effective in managing risks in a by the board approved manner.[45] The board should therefore consider the following factors:[46]

- the nature and extent of the risks facing the company;
- the extent and categories of risk which it regards as acceptable for the company to bear;
- the likelihood of the risks concerned materialising;
- the company's ability to reduce the incidence and impact on the business of risks that do materialise; and
- the costs of operating particular controls relative to the benefit thereby obtained in managing the related risks.

According to the Turnbull report management is responsible for implementing the board's policies on risk and control. Management should also provide the board with a balanced assessment of the significant risks and the effectiveness of the system of internal control in managing those risks.[47] The board itself should make a public statement on internal control and it should therefore undertake an annual assessment that should consider the changes in the nature and extent of significant risks, as well as the company's ability to respond to changes.

In the UK corporate governance rules and as an integrated part of it, the risk management system is regularly under review. The 2003 Higgs report stated that one of the key elements of the role of non-executives is risk management and that they must therefore check whether the systems of risk management are robust and defensible.[48] According to the Smith report, the audit committee – unless addressed by a separate risk committee or the board itself – should review the company's internal financial control and risk management systems. The audit committee should also assess the scope and effectiveness of these systems to identify, assess, manage and monitor financial and non-financial risks. Additionally, the audit committee should review and approve the internal financial control and risk management statements that are included in the annual report.[49] As a result, in July 2003 the Combined Code was revised by integrating the above-mentioned recommendations of the Higgs and Smith reports.[50] In 2003 the main principle regarding internal control sounded: 'The board should maintain a sound system of internal control to safeguard shareholders' investment and the company's

[45] Turnbull Committee, *Internal Control: Guidance for Directors on the Combined Code*(London: The Institute of Chartered Accountants in England & Wales (ICAEW), 1999 (Turnbull I Report)), Section 16.
[46] Turnbull I Report 1999, Section 17.
[47] Turnbull I Report 1999, Sections 18 and 30.
[48] Department of Trade and Industry, *Review of the role and effectiveness of non-executive directors* (2003 (Higgs I Report)), Chapters 4 and 6, p. 21 and p. 27.
[49] Financial Reporting Council (FRC), *Audit Committees – Combined Code Guidance* (2003 (Smith Report)), Chapter 2, Section 2.1 and Chapter 5, Sections 5.6 and 5.8, p. 6 and p.11.
[50] Financial Reporting Council (FRC), *The Combined Code on Corporate Governance* (2003 (Combined Code 2003)), Principle C.2 relates to internal control (former Principle D.2 of the Combined Code 2000). It only changed 'The review should cover all controls' into 'The review should cover all material controls'. See the supporting principles of Principle A.1 on p. 4 and Code provision C.3.2 on p. 16 of the Combined Code 2003 for the added recommendations of the Higgs I Report and Smith Report.

assets'.[51] It is the board's responsibility to annually review 'the effectiveness of the group's system of internal controls and should report to shareholders that they have done so. The review should cover all material controls, including financial, operational and compliance controls and risk management systems'.[52] This approach is confirmed in the Guidance on Audit Committees.[53] The previous interpretation of the City and the accounting profession that the requirement was limited to the internal financial controls was completely set aside.

In 2004 the independent Financial Reporting Council ordered a committee chaired by Douglas Flint to review the Turnbull guidance and to update it in light of the new national – combined code - and international – Sarbanes Oxley Act – developments. The revised Turnbull guidance of October 2005 is still applicable. The guidance refined the combined code principle and stressed that a sound internal control system facilitates the company's 'effective and efficient operation by enabling it to respond appropriately to significant business, operational, financial, compliance and other risks to achieving the company's objectives. This includes the safeguarding of assets from inappropriate use or from loss and fraud and ensuring that liabilities are identified and managed'.[54] The guidance acknowledges that good internal control contributes to safeguarding the shareholders' investment[55] but it does limit internal control to this objective. Testing the effectiveness of the internal control system is the board of director's responsibility.

The publication of the Walker Review of Corporate Governance in the UK Banking Industry in November 2009 raised questions as to whether the risk management systems and frameworks of the other industries also need a more modernized approach. The Financial Reporting Council acknowledged that further improvement of the internal control guidelines and reporting requirements is necessary, in particular regarding risk appetite assessment, tolerance and maintaining of the system.[56] The modernization is scheduled for 2010 and a first step was taken with the publication of the UK Corporate Governance Code in June 2010. The new main principle regarding internal control and risk management sounds: 'The board is responsible for determining the nature and extent of the significant risks it is willing to take in achieving its strategic objectives. The board should maintain sound risk management and internal control systems'[57]. The latest developments confirm and emphasize the policies which were already installed in the pre-financial crisis era.

In the mean time, the Department of Trade and Industry had set up a review of the entire company law, the Company Law Review, which resulted in the Companies Act 2006. The Act contains an important principle of director's behaviour in section 172:

---

[51] Main Principle C.2 of the Combined Code 2003.
[52] Code provision C.2.1. of the Combined Code 2003.
[53] Financial Reporting Council, *Guidance on Audit Committees* (London, October 2008), recommendation 4.6.
[54] Financial Reporting Council, *Internal Control – Revised Guidance for Directors on the Combined Code* (London, October 2005), p. 7.
[55] Ibid., p. 3.
[56] Financial Reporting Council, frc.org.uk/corporate/combinedcode.cfm, last consulted on 5 May 2010.
[57] Financial Reporting Council, *UK Corporate Governance Code* (London, June 2010), main principle C.2.

> A director of a company must act in the way he considers, in good faith, would be most likely to promote the success of the company for the benefit of its members as a whole, and in doing so have regard (amongst other matters) to
>
> (a) the likely consequences of any decision in the long term,
>
> (b) the interests of the company's employees,
>
> (c) the need to foster the company's business relationships with suppliers, customers and others,
>
> (d) the impact of the company's operations on the community and the environment,
>
> (e) the desirability of the company maintaining a reputation for high standards of business conduct, and
>
> (f) the need to act fairly as between members of the company.

Directors have to give appropriate weight to each of the different matters.[58] It can be summarized as the requirement to show socially responsible behaviour. Directors must also assess the risks of their acts. However, an overall principle to take into account all (external) risks is not provided. It follows from the obligation to provide a business review in which the directors must disclose the principal risks and uncertainties that at least a risk identification system must be in place.[59]

2.2.3. The Alternative French Approach

The French Companies Act – integrated in the Commercial Code – requires the board of directors to perform all controls and verifications that it considers expedient.[60] Since 2003 the chairman of the board of directors of a French listed entity or, in case the company is organized with a two tier structure, the chairman of the supervisory board must present a report to the general meeting of shareholders with the internal control procedures and the risk management established by and in the company. The report must highlight those procedures related to the gathering and treatment of the accounting and financial information both for the annual and the consolidated accounts. Like the implementation of the American Sarbanes-Oxley Act this French legal requirement caused companies many compliance difficulties in particular due to the lack of guidelines. The French supervisory authority Autorité des Marchés Financiers (AMF) revealed in its assessment of the first reports of the chairmen of over 100 large French companies that many reports failed to identify the field of application of the internal control system in place if any. The AMF also showed that less than half of the reports in the first year and only two thirds of the reports in the second year identified the major risks that companies were confronted with and which procedures were in place to mitigate these risks. Only a small minority of the reports indicated which internal control framework was applied. In addition only 10 per cent in the first year and one in four in the

[58] Rt Hon Lady Justice Arden DBE, 'Regulating the Conduct of Directors', *Journal of Corporate Law Studies* 2010, p. 7.
[59] Section 417 (3) Companies Act 2006.
[60] Article 225-35,section 3 of the French Commercial Code.

second year assessed the adequacy of the internal control procedures in place.[61] In light of these findings it is not a surprise that none of the reports refer to major shortcomings in the internal control framework. The AMF's analysis urged the regulator to issue an accompanying internal control and risk management framework. The French supervisory authority recommended the referential framework of the *Groupe De Place* which the AMF sponsored. This committee had to take into account the COSO framework as well as the pending proposals for European Directives regarding internal control. The report 'Le dispositif de Contrôle Interne: Cadre de référence' was published in 2006 and a *light* edition 'Cadre de référence du contrôle interne: Guide de mise en oeuvre pour les valeurs moyennes et petites' for small and medium sized listed companies was published in 2008.[62] Both reports clearly distinguished (reporting) requirements related to the general internal control framework and the more elaborated specific requirements with respect to the internal control over reporting of financial information. Next, the requirements are aligned but not identical to the COSO I report on internal control that includes an appropriate organizational structure, internal communication of information, a system to identify and manage the risks, control activities, and continuous monitoring. However, the French Commercial Code requires the chairman not only to report on the internal control procedures but also on risk management. Conversely and as opposed to the three objectives in COSO I, the French framework identifies four objectives which resembles the four objectives of COSO II, namely compliance, follow up of the instructions and the orientations of the executive board, good internal operations, in particular to protect the company's assets, and reliable financial information. The financial crisis did not (yet) change the French approach.

2.2.4. The Dutch in Control Method

The compliance with the Dutch Peters report was unsatisfactory and the Dutch Minister of Finance and Minister of Economic Affairs invited Euronext Amsterdam, the Employers Association and several other interested associations to develop a new corporate governance code, commonly known as the Tabaksblat Code. It was issued in 2003 and at the end of 2004 the code and its comply or explain regime was legally acknowledged. The main internal control and risk management provisions are set out in principle II.1 of the Tabaksblat Code. The principle deals with the responsibility of the management board for complying with laws and regulations, managing the risks associated with the company's activities, and financing the company. Furthermore, it stipulates that the management board has to report related developments to and discuss the internal risk management and control systems with the supervisory board and its audit committee. The best practice provisions required the management board to[63]:

---

[61] AMF, *Rapport AMF 2005 sur le governenement d'entreprises et le contrôle interne* (Paris, January 2006), p. 22.

[62] Both reports can be downloaded from amf-frace.org.

[63] Tabaksblat Committee (Corporate Governance Committee), *The Dutch corporate governance code: Principles of good corporate governance and best practice provisions*, (2003 (Tabaksblat Code)), Best practice provisions II.1.3 and II.1.4, p. 9.

> II.1.3 […]have an internal risk management and control system that is suitable for the company. It shall, in any event, employ as instruments of the internal risk management and control system: (a) risk analyses of the operational and financial objectives of the company; (b) a code of conduct which should, in any event, be published on the company's website; (c) guides for the layout of the financial reports and the procedures to be followed in drawing up the reports; and (d) a system of monitoring and reporting.
>
> II.1.4 […]declare in the annual report that the internal risk management and control systems are adequate and effective and shall provide clear substantiation of this. In the annual report, the management board shall report on the operation of the internal risk management and control system during the year under review. In doing so, it shall describe any significant changes that have been made and any major improvements that are planned, and shall confirm that they have been discussed with the audit committee and the supervisory board.

The latter best practice provision is commonly known as the *in control statement*. It is also best practice that the supervisory board monitors:[64]

(i) achievement of the company's objectives:
(ii) corporate strategy and the risks inherent in the business activities;
(iii) the structure and operation of the internal risk management and control systems;
(iv) the financial reporting process;
(v) compliance with the legislation and regulations.

Like in France where the AMF annually assesses companies' reporting on corporate governance and internal control, the Dutch monitoring commission annually analyzed corporate governance reporting. The aforementioned requirements were, like in France, not accompanied with a (recommendation of a) framework which could provide Dutch companies the necessary guidance in particular with respect to *effectivity* and *adequacy*. The monitoring commission first provided guidelines to comply with the financial reporting risks and the other – operational, strategic and compliance – risks. It also offered good practices to portray the risk profile and the internal control and risk management system in the in control statement. The commission also emphasized that Dutch companies with a dual listing on an American stock exchange that have to comply with SOX are also compliant with the Dutch regulatory framework.[65] This explanation was surprising as the SOX requirements are limited to the maintenance and effectiveness of an adequate internal control structure and procedures for financial reporting. The proposals have been incorporated in the new edition of the Dutch Corporate Governance Code of 2008 (DCGC 2008). The DCGC 2008 requires companies to have an internal risk management and control system suitable for the company with, as

[64] Ibid., Best practice provisions II.1.6, p. 16.
[65] Monitoring Commission Corporate Governance, *Rapport over de evaluatie en actualisering van de Nederlandse corporate governance code*, June 2008, pp. 43-46.

instruments of the system, risk analyses of the company's operational and financial objectives and a monitoring and reporting system.[66] Besides being responsible for complying with all relevant primary and secondary legislation and managing the risks associated with the company's activities, the management board is also responsible for the company's risk profile. In line with the Tabaksblat Code, the management board has to report related developments to and discuss the internal risk management and control systems with the supervisory board and the audit committee.[67] The DCGC 2008 has amended the in control statement by requiring the management board to declare in the annual report that the systems provide a reasonable assurance that the financial reporting does not contain any errors of material importance and that the systems have worked properly.[68] Thus, instead of declaring that the systems are adequate and effective, the management board has to declare that the system provides reasonable assurance, which is a major reduction of the requirement. Since 2009 the declaration only has to address the financial reporting – not other aspects of the system such as strategy, operations and compliance – and only for errors of material importance. However, The DCGC 2008 added a provision requiring the management board to give a description in the annual report of: (1) the main risks related to the strategy of the company; (2) the design and effectiveness of the internal risk management and control systems for the main risks during the financial year; and (3) any major failings in the internal risk management and control systems, including significant changes made to the systems and the major improvements planned, and a confirmation that these issues have been discussed with the audit committee and the supervisory board.[69] The system set out by the COSO reports is cited as an example of an internal control and risk management system in the explanatory statement.[70] Also, the DCGC 2008 provides that the supervisory board's oversight of the management board has to include the company's risks inherent to the business activities and the design and effectiveness of the internal risk management and control systems.[71] One of the key committees of the supervisory board, the audit committee, has to monitor the activities of the management board with respect to the operation of the internal risk management and control systems.[72]

In light of the financial crisis the DCGC will not be strengthened. However, like in the UK, a new Banking Code was issued in September 2009.[73] It is applicable on all Dutch licensed banks. The code provides in a risk appetite approval and risk monitoring procedure as well as a product approval process. A risk committee must assist the supervisory board in its risk

[66] Corporate Governance Code Monitoring Committee, *The Dutch Corporate Governance Code – Principles of Good Corporate Governance and Best Practice Provisions*, 2008 (2008 DCGC), Best practice provision II.1.3.
[67] Ibid., Principle II.1.
[68] Ibid., Best practice provision II.1.5.
[69] Ibid., Best practice provision II.1.4.
[70] See the 'Explanation of and notes to certain terms used in the code' of the DCGC 2008, p. 39 and of the Tabaksblat Code 2003, p. 33.
[71] Ibid., Best practice provision III.1.6.
[72] Ibid., Best practice provision III.5.4.
[73] NVB, *Banking Code*, September 2009, p. 16.

monitoring role. It is expected that the comply or explain code will be legally endorsed. In the mean time a monitoring commission assesses the compliance with the Banking Code.[74]

2.2.5. The German and Belgium Follow Up

Above it was shown that Germany was the first Western European country that legally endorsed a specific risk management system, the *Frühwarnsystem*. Conversely, Germany was very late in the development of a generally accepted corporate governance code. Only in 2000 a Government Panel on Corporate Governance was installed. It reported to the German chancellor in July 2001 after which the German Minister of Justice installed a corporate governance commission. The code was published in 2002 and obtained the status of a mandatory comply or explain code via section 161 of the German Companies Act. It did not contain many guidelines regarding internal control or risk management. It explicitly recognizes the management board's responsibility for risk management and the requirement for the chairman of the management board to discuss risk management with the chairman of the supervisory board. The audit committee must 'handle issues of accounting and risk management'.[75] In the 2005 edition the commission added that the chairman of this committee must have knowledge of and experience in internal control processes.[76] Other or more detailed governance regulations are not included in the code.
The 2009 edition introduced an new guideline: 'The Management Board is responsible for independently managing the enterprise with the objective of sustainable creation of value and in the interest of the enterprise, thus taking into account the interests of the shareholders, its employees and other stakeholders'.[77] The guideline is not as stringent as section 172 of the UK Companies Act but social responsibility is explicitly recognized in this stakeholder oriented country. The financial crisis did not yet result in more specific risk management guidelines in the code.

Finally, Belgium followed the developments in these and other countries. When Germany and the Netherlands issued new corporate governance codes which were provided with a legal comply or explain status, Belgium established a corporate governance commission that issued its code late 2004. It contained several internal control and risk management related provisions and guidelines. First, it is explicitly acknowledged that the board is responsible to enable the company to identify and to manage its risks and to define its risk appetite.[78] The board must ascertain that an internal control system that effectively identifies and manages risks including the compliance risks of which the effectiveness must be controlled by the audit committee, is in place. The executive management must establish internal controls for all different kinds of risks.[79] Like the UK 2003 Smith report the Belgian code recommends in a

[74] J. De Jager, Letter of the Minister of Finance, 24 March 2010, p. 2 (www.dnb.nl/openboek/extern/file/dnb_tcm40-197407.pdf)
[75] Government Commission, *German Corporate Governance Code*, 2002, provisions 4.1.4., 5.2, and 5.3.2..
[76] Government Commission, *German Corporate Governance Code*, 2005, provision 5.3.2..
[77] Government Commission, *German Corporate Governance Code*, 2009, provision 4.1.1..
[78] Belgian Commission Corporate Governance, *The Belgian Code on Corporate Governance*, 2004, provision 1.1 and provision 1.2.
[79] Ibid., provision 1.3., 6.5 and 5.2/7.

guideline an induction programme for its audit committee members. This programme must provide an overview of the company's internal control organization and risk management systems.

According to the industry and a number of scientific studies the Belgian corporate governance code was well received. However, it is our understanding that these studies do not analyze the functioning of the internal control systems. Therefore, it does not come as a surprise that the 2009 update of the code hardly changed the recommendations on internal control and risk management systems. In the 2009 edition the board of directors must approve and assess the implementation of the internal control and risk management framework.[80] The most important characteristics of the framework must be disclosed in the corporate governance statement, a European disclosure requirement which is recently endorsed by a new corporate governance law.[81] Furthermore, not only for the members of the audit committee but for all board members an induction programme with the fundamentals of risk management and internal control must be provided.[82]

3. Risk Management and Internal Control in Practice

3.1. Research Design

To gain proper insight in the identification, assessment, response and control of risks and risk management systems before and after the financial crisis, an analysis of risk management reporting in the annual reports of 2000, 2005 and 2009 of five real estate companies in the five different countries is performed. The year 2000 is selected as the year before the explosion of corporate scandals and accounting irregularities that burst over the financial markets late 2001 and 2002. By 2005 both regulators and companies had sufficient time to mitigate the problems that the crisis of the start of the millennium caused. Finally, in their 2009 report companies had the opportunity to address the consequences of the financial crisis. The companies in the sample are: Wereldhave (The Netherlands), Cofinimmo (Belgium), British Land (UK), Unibail-Rodamco (France) and IVG Immobilien (Germany). These companies specialize in property management and property development. Wereldhave, Unibail and Cofinimmo strategically focus on the first. Over the years IVG Immobilien oriented towards the development of real estate investment products, but property management remained its core business. British Land specializes in the second activity. As a consequence operational risk management of British Land has different priorities.

[80] Belgian Commission Corporate Governance, *The Belgian Code on Corporate Governance*, 2009, provision 1.3.
[81] Law of 6 April 2010 tot versterking van het deugdelijk bestuur bij de genoteerde vennootschappen en de autonome overheidsbedrijven en tot wijziging van de regeling inzake het beroepsverbod in de banken financiële sector, *Official Gazette* 23 April 2010, p. 22709.
[82] Belgian Commission Corporate Governance, *The Belgian Code on Corporate Governance*, 2009, provision 4.8.

The focus of this analysis is on the risk management report or provisions in the business review or corporate governance statement, and less on the risk reporting in the notes to the accounts. According to the COSO II framework, the risk management process should be divided in the following activities: set the internal environment, objective setting (risk appetite), event identification, risk assessment, risk response, control activities, information and communication and monitoring the effectiveness. The annual report does not provide information on all the different activities. We limit the analysis of the annual reports to the event identification, the risk assessment, the risk response and monitoring. The review illustrates the level of information that is publicly disclosed via the annual report. The risk management part of the annual report is provided in a narrative report.[83] It goes without saying that the sample of the survey is too small to be representative for all companies. Further the reported results could be flawed as there is a considerable risk that the surveyed reports only partially report on the practices in place. Notwithstanding these restrictions the results of the analysis can be summarized as follows.

3.2. Research Results

First, according the amendment of the fourth and seventh company law directive, companies must disclose the main features of the risk management and internal control system for financial reporting in the corporate governance statement. Notwithstanding the fact that the law limits the requirement to financial reporting, an efficient system obliges the integration of this internal control system into a broader and general risk management system. All companies reported in 2009 on the use of a – national – internal control system. Whilst the French company Unibail-Rodamco applied the AMF framework and British Land referred to the use of Turnbull, IVG developed an adjusted accounting related internal control system, Wereldhave did not identify any framework but stressed the appropriateness of its internal administrative organization. Only Cofinimmo explicitly acknowledged the use of COSO. The reference to the use of a framework is accompanied with the use of a code of conduct or ethical guidelines and/or a compliance guide.

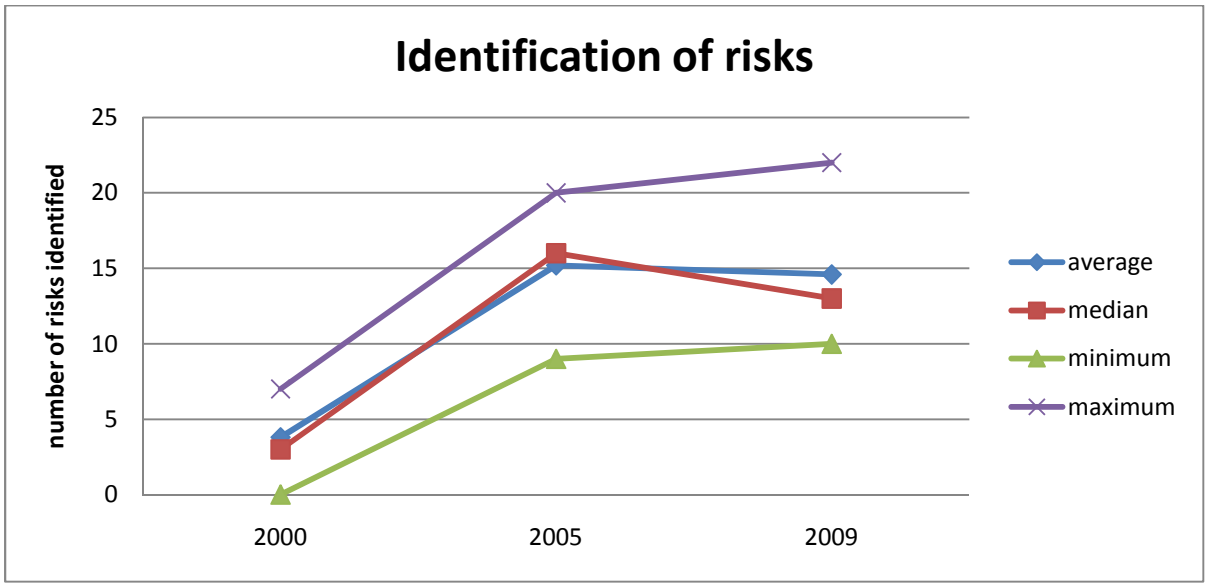
The explicit identification of the framework is obviously related to the legal developments. In 2000 only British Land and IVG referred to the use of a control system, the former to the Turnbull report, published in 1999, the latter via an overview of the different steps of identifying, assessing, managing and monitoring risks. In 2005 Unibail provided the report of the chairman of the board describing the use of a – non-identified – internal control system and Wereldhave referred to a non-identified internal control system to meet the requirements of the Tabaksblat code. In 2009 all companies apply an internal control framework.

Key is the identification of the portfolio of the events a business is confronted with. Due to the regulatory requirements and business strategy, only negative events – risks – are described in detail in the annual reports. In 2000 only the largest company and IVG for which the early warning system was already mandatory, identified and reported some (financial) risks. The

[83] British Land PLC provides the principal risks, the impact and the responses in a table. However the identified risks were requalified to fit into table 2 (like the financial market development which the company has split in two risks, was merged into one risk in table 2).

major turnaround took place during the first part of the millennium. Even in countries where the regulatory requirements regarding (the reporting of) risk management were installed after 2005, like in Belgium, companies invested in risk management systems. In the second half of the decade the systems were further improved, aligned with the regulatory requirements and consolidated. Since 2005 the average number of reported risks stabilized around 15, with a minimum around 10 and a maximum around 20 (figure 1). A first analysis of all listed real estate investment funds in the Netherlands supported these findings; the annual reports refer to 16 risks on average, with a minimum of 13 and a maximum of 20.[84]

Figure 1



source: own research based on annual reports

The development of reporting on risks coincided with the interest for and requirement to manage these risks. For a long period of time only financial risk management was emphasized. In 2000 the majority of the companies only identified currency, interest and liquidity risk. By 2005 all companies identified these financial risks and the majority added a list of operational and strategic risks. The other identified risks were more of an idiosyncratic nature.

According to COSO, risk assessment is the fourth important step in the risk management process. Each risk must be classified according to its impact on the objectives of the company and likelihood of occurrence. Risk assessment employs both qualitative and quantitative methods. Risk assessment reporting suffers from the difficulties to standardize qualitative methods. While no assessment reporting could be found in the annual reports of 2000, in 2005 the impact of the financial risks was well documented. Both in 2005 and in 2009 most companies quantitatively documented the impact of the volatility of currencies and interests.

[84] The detailed results are on file with the author.

In a number of 2009 reports this information was completed with the assessment of the impact of operational risks, like the exposure to contract termination and the default of tenants.

The likelihood of occurrence is barely reported. As a result, classification of risks categories in order of importance is missing in all reports. It creates a field of tension between the appearance of compliance with a referential framework and the state of the art of the risk management system.

According to COSO there are four types of risk response: acceptance, avoidance, sharing and reduction. In case of acceptance, the company must monitor the risk, for the reduction of risks controls are necessary while insurance is the most common technique for risk sharing. Most companies combine all four types of responses although information on avoidance is missing: as the company eliminates the risk by getting out of the situation hardly any information is provided. An exception to this rule is the currency risk. Some companies have developed their business in the Eurozone and are not confronted with the currency risk. Table 1 provides an overview of the most common risk responses of real estate investment companies. While strategic risks are monitored and financial risks are reduced, the other types of risks are more actively managed via different techniques of controls, risk sharing and monitoring. A relative new phenomenon is the monitoring of the reduction techniques of financial risks. Most companies recently started to provide information on the quality of the counterparty of the derivatives.

There is no ranking of the different kinds of risk responses and investors and other stakeholders have to assess the appropriateness of the risk response. While some companies opt for fixed interest rate loans to mitigate the interest rate developments, others explicitly selected variable interest loans to profit from these developments. Stakeholders must examine the market developments to assess the risk response of each company. Similarly, some companies adopted a policy of spreading the (tenant) counterparty risk as much as possible, whilst others concentrate this risk to mitigate more cumbersome administrative procedures of tenants' compliance.

Information of the control activities and the effectiveness testing of the system is underdeveloped. In general, responsibility of the management and the audit committee is assumed and some companies have installed an internal audit function. However companies do not frequently address questions on the feasibility of the risk management systems and the deficiencies of the system are not disclosed. However, companies regularly report improvements of the systems, indirectly indicating the weaknesses of the previous system. One of the companies reported that in 2009 a risk inventory on the basis of individual risks was carried out for the first time, clearly illustrating the weaknesses of the previous system.

Table 1: Risks and risk responses of real estate companies

Risk class	Risk	Risk response class	Risk responses					
Strategic and REIT status		accept	monitoring by the board	quarterly assessment finance department				
Operations (and economic)								
	market development	accept	monitoring	developing new properties	sell older properties	long contract terms	maintenance programs	
	lease price	accept/reduce	developing new properties	sell older properties	long term leases	maintenance programs	prime locations	
	letting	reduce	follow up tenants	regular contacts with tenants	active letting campaigns			
	property valuation	reduce/sharing	internal valuation (quarterly or semi-annual)	external valuation (quarterly or semi-annual)	insurance			
	counterparty (tenants)	reduce/sharing	advance payments	(bank) guarantees	pre-letting screening	diversified tenant	reputed tenants	follow up of tenants
	real estate development	reduce	close supply chain relationships	well developed project management	first class contractors	due diligence for acquisitions		
Finance								
	currency	reduce	matching	hedging	use of financial derivatives	ALM committee		
	interest	reduce	fixed interest loans	variable interest loans	use of financial derivatives	ALM committee		
	refinancing	reduce	different bank relationships	credit facilities	reputed banks	solid solvency ratio		

	financial instruments	reduce	monitoring credit exposure to derivatives	banks with credit rating		
	liquidity risk	reduce	maturities spread in time	financing facilities	monitoring covenants	cash management
Legal						
	regulations and administrative procedures	accept	monitoring	local companies		
Other						
	fraud and misstatement	accept/reduce	transparancy	segregation of duties	well organised administrative organisation	
	construction health and safety/environment	sharing	requirements on contractors	environmental code	energy efficient constructing	

4. Discussion and Conclusion

For a long period of time risk management was considered a financial, a reporting or - at best - an operational issue. Middle management deemed to mitigate the impact of unexpected financial market developments, in particular the interest rates or exchange rates via different financial hedging arrangements. In operations many companies spend significant resources to optimize supply, to limit industrial accidents, to improve IT-support, and so on. The European Union endorsed the harmonization of financial reporting obliging companies to develop an appropriate financial administrative system.

However, the last fifteen years risk management and internal control developed into a pivotal element of good corporate governance. All corporate governance codes in Western Europe refer to the implementation of and maintaining internal control and risk management systems as best practice. This development coincided with the growth of legal requirements to establish risk management systems, in particular systems in relation to the financial reporting process. It shifted the interest and awareness to the top levels of the company, including the board of directors, the audit committee and the external auditor.

The major efforts to raise the standards of accountability for risk management have spurred the harmonization of systems and procedures. In many countries new risk management responsibilities were followed by frameworks to help companies to implement the requirements. In the UK and France the work of the Turnbull committee and the *Groupe de Place* commission provided helpful insights in the translation of the recommendations in applicable tools. In other countries the interaction of the regulators with the business community reduced the gap between the regulatory expectations and the business capacities to provide in risk management. In the Netherlands the in control statement must now provide *reasonable assurance* instead of "the statement of an adequate and effective system".

The harmonization of the regulatory frameworks is visible in corporate reporting of risk management. In 2000 risk management reporting was, at best, fragmented. In 2009 all companies have included a risk management section and describe in detail the risks and risk responses. Reporting and probably implementation of risk management systems still suffer from vagueness and fragmentation of the regulatory framework. Financial risks are quantified and well addressed, the other types of risks are at best qualified and some companies start with scenario analysis to evaluate the impact of the risks incurred. The latter development must be encouraged to integrate the different risks in the risk management approach.

The regulatory integration of risk management and internal control in the corporate legal framework is still fragmented and incomplete. Despite the harmonization efforts some areas require more detailed study. At the moment many rules foresee an obligation to install and maintain both internal control *and* risk management systems. However, COSO II explicitly acknowledged the incorporation of the internal control framework in the enterprise risk framework to move forward to a mature risk management process. Many regulators refer to COSO as an appropriate framework for companies to comply with the legislative and/or

regulatory requirements. It is an open question which COSO framework meets the minimum standards avoiding liability and which degree of compliance is required to meet these obligations. The lack of clarity is also visible in the systematization of the regulatory objectives. According to some regulatory bodies it is sufficient if the systems provide reasonable assurance regarding the reliability of the financial reporting process, whilst others require that the corporations provide in processes that all the objectives can be achieved: strategic, operational, compliance and reporting objectives. It illustrates that the legal requirements as well as the eagerness of companies to fully comply – or at least report full compliance - with all best practices create a field of tension between the basic assumption of risk management frameworks in providing (only) reasonable assurance and the (reported) state of the art of managing and presumably controlling all (material) risk.

The mandatory requirements to establish and maintain internal control and risk management systems concurred with the identification of concerned corporate parties who are accountable for setting up and maintaining the systems. Parliaments all over Europe and at the European level identified the responsibilities of the audit committee, the (supervisory and management) board, the executive management, like the senior accounting officer according to schedule 46 of the UK Finance Act 2009 and the external auditor. In corporate governance codes other constituents, like the internal audit department, risk officers, compliance officers and other officers and employees were provided with responsibilities regarding (parts of) the day-to-day operations of the systems.[85] Whilst responsibilities of most corporate constituents have been more or less clearly identified, other aspects of (corporate) law have not been fully addressed. An important feature of a directorship and the board of directors in many jurisdictions is the independence to make the appropriate decisions. The board is accountable to the general meeting of shareholders, and the company law framework provides the board and its members with the power to run the company (in the interest of all corporate constituents or in the interest of the shareholders depending on the view defended).[86] If directors are entrusted with the functions of risk manager or compliance officer, corporate law is providing adequate tools to mitigate the conflicts between independence in mind, independence in appearance and independence in fact. However, often the chief accounting officer, the compliance officer and risk management officer are not directors but officers subjected to the authority of the board. As employees of the company they have to work under the authority, the direction and supervision of the board of directors. At least the independence in appearance is affected and often independence in fact will be difficult to support. Balancing the trade off between the independence and the accountability and responsibility is a very difficult exercise in labour relationships.

Another, even more important issue, is the relationship between responsibility and liability regarding the new requirements to establish and maintain internal control and risk management systems. The European Directive 2006/46/EC explicitly acknowledged the

---

[85] See eg. "All employees have some responsibility for internal control as part of their accountability for achieving objectives"(Financial Reporting Council, *Internal Control – Revised Guidance for Directors on the Combined Code* (London, October 2005), p. 6).

[86] For a recent overview of the position and role of the board in a number of countries see B. Sjafjell, *Towards a Sustainable European Company Law*, European Company Law Series, (Kluwer Law International: Alphen aan den Rijn 2009), p. 45-63.

collective responsibility and liability of the different boards for the accounts, the annual report and the corporate statement. However, for all other duties liability is not further specified. National and general liability rules prevail, which boils down to the liability of the board for mismanagement and officers for breach of contract. In view of the new responsibilities and corporate governance developments board of directors, more than ever before, sets up specialized subcommittees and consists out of separate classes of directors. Especially the audit committee is considered as an important subcommittee in European member states. The members of the audit committee bear important corporate responsibilities as regards the effectiveness of the risk management systems. However, in some countries (all) the directors are jointly and severally liable vis-à-vis the company as well as vis-à-vis third parties for any loss resulting from an infringement of the provisions of the Companies Act.[87] Any kind of division of liability between audit committee directors and other directors is lacking. It also raises questions as to the duties of the other directors regarding the monitoring of the work of the audit committee. The mature responsibility status that these committees acquired, does not (yet) correspond with the corporate liability frameworks that still date from the pre-risk management periods.

Officers must perform in accordance with the principles of good faith, due care and equity. In several jurisdictions they are liable for damages vis-à-vis the company and even third parties. In light of the new internal control and risk management responsibilities, modifications of the working conditions will not only require an appropriate board mechanism to make use of the "ius variandi" but also fleshing out the accountability of officers vis-à-vis developing risk management. Risk appetite, tone at the top and strategy are dynamic concepts which have to fit into the static labour relationships as regards the liability of the officers. Boards can unilaterally change the strategy or tone at the top which the officer must implement, apply and adhere to. It is the duty of the board of directors to develop policies. This duty is accompanied with the right (and duty) of the individual director to react and respond and ultimately (the duty) to resign in case of insurmountable disagreement. These rights and duties are – to say the least – less evident in the position of an officer who works under the authority and supervision of the board. A recent decision of the German *Bundesgerichtshof* of 17 July 2009[88] which found the compliance officer guilty and referred to a criminal "Garantenpflicht"[89] of this officer shows a reflection is required.

[87] See for example article 528 Belgian Companies Code. Directors who had no part in the infringement must act in compliance with a specific procedure to be exempted from liability.
[88] S. Mutter and D. Quincke, 'Vorstand und Aufsichtsrat – Garantenstellung bei pflichtwidriger Compliance', *Die Aktiengesellschaft* (2009), R 416-R418.
[89] 'duty to guarantee'.

about ECGI

The European Corporate Governance Institute has been established to improve *corporate governance through fostering independent scientific research and related activities.*

The ECGI will produce and disseminate high quality research while remaining close to the concerns and interests of corporate, financial and public policy makers. It will draw on the expertise of scholars from numerous countries and bring together a critical mass of expertise and interest to bear on this important subject.

The views expressed in this working paper are those of the authors, not those of the ECGI or its members.

ECGI Working Paper Series in Law

Financial assistance for the services of the editorial assistant of these series is provided by the European Commission through its RTN Programme on European Corporate Governance Training Network (Contract no. MRTN-CT-2004-504799).

Electronic Access to the Working Paper Series

The full set of ECGI working papers can be accessed through the Institute's Web-site (www.ecgi.org/wp) or SSRN:

Finance Paper Series	http://www.ssrn.com/link/ECGI-Fin.html
Law Paper Series	http://www.ssrn.com/link/ECGI-Law.html