# Financial Law Institute

Working Paper Series

**WP 2013-02**

**Christoph VAN DER ELST**

**The Risk Management Duties of the Board of Directors**

May 2013

WP 2013-02

Christoph VAN DER ELST

# The Risk Management Duties of the Board of Directors

## Abstract

The board of directors is responsible for an appropriate business risk management environment. The paper studies in a comparative way how legislators and courts fill this duty. We question whether the legislative and regulatory framework will improve the equilibrium between entrepreneurship and risk control. We advocate for a distinct approach for strategic and operational risk management, defining risk appetite and tolerance and sufficient monitoring. We also call for full and detailed reporting and compliance risk management.

# The Risk Management Duties of the Board of Directors

Christoph Van der Elst

Tilburg and Gent University, ECGI

*To be published in Hanne Birkmose, Mette Neville & Karsten Engsig Sørensen (eds.), Boards of Directors in European Companies – Reshaping and Harmonising Their Organisation and Duties, Forthcoming*

Recently, many companies, shareholders and society have had to spend billions of dollars to restore damage from management failures. The oil spill in the Gulf of Mexico, the alleged Goldman Sachs' fraudulent structuring and marketing of synthetic mortgage bonds, the (continuation of) skyrocketing bonus schemes, etc., had an enormous impact on the economy and started a call for the assessment and management of companies' exposure to risks. All companies must be equipped with appropriate procedures addressing these risks and preventing new catastrophes to happen. The board of directors should be responsible for the continuity of the business, timely identify harmful events and take responsible action. This chapter addresses what this call for risk management resulted in and whether it can equilibrate corporate venturing and risk control. The first section sketches the fiduciary duties of the board of directors. Next, specific business compliance requirements are addressed in section two. The third section provides insight in the new regulatory risk management environment in Europe, both from the European perspective and from the perspective of a selection of national Member States. Legislators and regulators issued a patchwork of laws and rules to manage risk. It also provides insight in the (new) risk management components and systems. In the fourth section it is studied how courts approach these new risk management provisions. In the last section we question whether the new legislative and regulatory framework will improve the equilibrium between entrepreneurship and risk control. We advocate for a distinct approach for strategic and operational risk management, defining risk appetite and tolerance and sufficient monitoring and for full and detailed reporting and compliance risk management.

1. Fiduciary Duties

According to most company legislations the board of directors is entrusted with the management of the company and it is accountable to the company and its shareholders for this management. In former 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'[1]. According to the Dutch, Belgian and French Codes it was, and still is, the duty of the board of directors to govern the company.[2] In the two-tier German structure the management board is responsible for the management of the company and the supervisory board must monitor the management of the companies.[3] An article or section regarding the representation of the company follows this management duty.[4]

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[5] or, like in Finland, to see to the administration of the company and the appropriate organization of its operations.[6] In other countries, like the UK, it is fine-tuned as a duty to act in the way the director 'considers, in good faith, would be most likely to promote the success of the company for the benefit of its members as a whole'[7]. In particular in large companies company law recognizes that this responsibility to govern the company is delegated to the management. Under the Delaware General Corporation Law it is provided that the company is either 'managed by or under the direction of a board of directors'[8]. Especially in larger companies the primary responsibility of the directors is to oversee the affairs of the company for the benefit of the company and its shareholders or stakeholders.

Corporate law offers many degrees of freedom for the board of directors implementing governance strategies. The duties of the board were not defined in company law in further detail and the standards of conduct were assessed ex post by the courts when something went

[1] Regulation 70 of the UK 1985 Table A. The Companies Act 1985 is less precise and only provides that the duty of the directors is owed to the company (section 309(2) CA 1985).
[2] Book 2:129 Dutch Civil Code, Article 53, Belgian Companies Act 1935 and Article 89, French Companies Code 1966.
[3] Article 76(1) and Article 111(1) German Stock Corporation Act 1965.
[4] 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).
[5] Book 2:9 Dutch Civil Code.
[6] Chapter 6, section 2 (1) Finnish Companies Act.
[7] Section 172 Companies Act 2006.
[8] Section 141 (a).

wrong.[9] In the US these fiduciary duties boil down to two types of duties: the duty of care and the duty of loyalty. The duty of loyalty requires directors to subordinate their personal interests to those of the company and applies in particular when the director has a material (financial) interest in a transaction at odds with the interests with the company.[10] The directors must also comply with the duty of care when they make decisions. Business judgment requires from directors that 'in making a business decision, the directors of a corporation acted on an informed basis, in good faith and in the honest belief that the action taken was in the best interests of the company'[11]. The board of directors will not be liable if they informed themselves 'prior to making a business decision, of all material information reasonably available to them'[12]. The Delaware Supreme Court uses the concept of gross negligence as 'the proper standard for determining whether a business judgment reached by a board of directors was an informed one'[13]. In the Re Caremark case Chancellor Allen made it clear 'that a director's obligation includes a duty to attempt in good faith to assure that a corporate information and reporting system, which the board concludes is adequate, exists, and that failure to do so under some circumstances may, in theory at least, render a director liable for losses caused by non-compliance with applicable legal standards'[14]. In Stone v. Ritter the Delaware Court confirmed that liability follows from conscious disregarding the board's duties[15] and the Citigroup case proved that the Delaware court judges business decisions that in hindsight turned out poorly for the company cannot be equated to breaching the fiduciary duty of care.[16]

The American duty of care implies that the directors must make sure that an information and reporting system is in place. In legal literature these requirements are explained as the duty to establish an oversight system including risk assessment and risk management.[17] While

[9] For a recent overview of the developments of fiduciary duties, see C. Hill and B. McDonnel, *Fiduciary Duties: The Emerging Jurisprudence*, in *Research Handbook on the Economics of Corporate Law*, C. Hill and B. McDonnel (eds.), 133-151 (Edward Elgar, 2012). A recent overview of the monitoring duty can be found in J. Hill, *Centro and the Monitoring Board – Legal Duties versus aspirational Ideals in Corporate Governance*, UNSW, 341-359 (2012) and E. Pan, *A Board's Duty to Monitor*, NY Law School Law Review, 718-740 (2009-2010).

[10] Model Business Corporation Act §8.60 (1).

[11] *Aronson v. Lewis*, 473 A.2d 805 (Del. 1984) at 812.

[12] *Ibid*.

[13] *Smith v. Van Gorkum*, 488 A.2d 858 (Del. 1985).

[14] *In Re Caremark International Inc. Derivative Litigation* 698 A.2d 970 (Del.Ch. 1996).

[15] *Stone v. Ritter*, 911 A 2d 362 (Del. 2006).

[16] *In re Citigroup Inc. Shareholder Litig.*, 2009 WL 481906 (Del. Ch. 2009).

[17] K. Johnson, *Addressing Gaps in the Dodd-Frank Act: Directors' Risk Management Oversight Obligations*, University of Michigan Journal of Law Reform, 82 (2011); R. Miller,

directors will only be liable if directors 'utterly failed to implement any reporting or information system or controls', it is argued that the directors must ensure that a risk management system is in place. In the Citigroup case it is recognized that the board of directors can be held liable for 'a failure to monitor business risk'[18]

2. Specific Industry, Activity, and Compliance Requirements

The overall responsibility of directors for monitoring the company's business affairs and the provision of a risk management system are accompanied with many specific additional industry related obligations, specific activity related requisites and compliance requirements. In the pharmaceutical industry the entity that places a medicinal product on the market must provide for a risk management system defined as 'a set of pharmacovigilance activities and interventions designed to identify, characterize, prevent or minimize risks relating to a medicinal product, including the assessment of the effectiveness of those activities and interventions'[19] and described in the 'risk management plan'. In the chemical industry 'companies must identify and manage the risks linked to the substances they manufacture and market in the EU. They have to demonstrate to the European Chemical Agency how the substance can be safely used, and they must communicate the risk management measures to the users'[20]. Credit institutions must have 'robust governance arrangements, which include a clear organizational structure with well-defined, transparent and consistent lines of responsibility, effective processes to identify, manage, monitor and report the risks it is or might be exposed to, adequate internal control mechanisms, including sound administration and accounting procedures, and remuneration policies and practices that are consistent with and promote sound and effective risk management'[21]. The remuneration policies of the credit

---

*Oversight Liability for Risk Management Failures at Financial Firms*, Southern California Law Review, 90 (2010).

[18] *In re Citigroup Inc. Shareholder Litig.*, 2009 WL 481906 (Del. Ch. 2009). An analysis of the risk management role of the board of directors in the European banking industry see E. Wymeersch, *Risk in financial institutions – is it managed?* FLI working paper 2012/4, 13 p. (2012)

[19] Article 1, 28b. of Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use, *OJ* L nr. 311, 28 November 2001, p. 67 (Consolidated version of 21 July 2011).

[20] http://echa.europa.eu/web/guest/regulations/reach/understanding-reach (accessed February 1, 2013).

[21] Article 1.3, amending article 22 Directive 2006/48/EC of D**irective 2010/76/EU of the European Parliament and of the Council of 24 November 2010 amending Directives**

institutions should take into account the risk management systems and prevent 'risk-taking that exceeds the level of tolerated risk of the credit institution'[22].

Next to specific rules that are applicable in many industries, boards of directors must comply with additional rules if certain activities are developed, even if the business activities are situated in other industries. Any business that produces, processes or distributes food must provide for food safety. All stages of production, processing and distribution of food processes must be designed and constructed to avoid the risk of contamination. Thereto the food business operators must have 'in place, implement and maintain a permanent procedure or procedures based on the HACCP principles'[23], the Hazard Analysis and Critical Control Point (HACCP) principles provide for reasonable insurance for safe food.

Third, many businesses are submitted to generic compliance requirements, often enforced though liability claims against the board of directors. The famous American risk management SOX legislation requires in section 301 that 'each audit committee shall establish procedures for (A) the receipt, retention, and treatment of complaints received by the issuer regarding accounting, internal accounting controls, or auditing matters; and (B) the confidential, anonymous submission by employees of the issuer of concerns regarding questionable accounting or auditing matters'.

The general rule of fiduciary duties and the different layers of specific internal control, risk management and compliance requirements could not prevent a tumultuous start of the new millennium. Financial risk management and corporate governance scandals were not new. In the nineties several major debacles were reported in the financial press. To name but a few in 1991 Robert Maxwell was, against the pension fund rules in place, pledging pension fund assets for the financing of less successful activities of the group. When Maxwell unexpectedly died in November 1991 the misconduct was discovered, and it was found out that the debt of the companies was more than an unbearable USD 1 billion.[24] In 1993 a subsidiary of Metallgesellschaft engaged in too many long-term forward contracts and covered its position

---

**2006/48/EC and 2006/49/EC as regards capital requirements for the trading book and for re-securitizations, and the supervisory review of remuneration policies Text with EEA relevance, *OJ** *L No 329 of 14 December 2010, p. 3. At the moment of writing this Directive is under revision (proposal for a CRD IV) and it can be expected that the requirements vis-à-vis risk management will be further strengthened.*

[22] Annex I (1) of Directive 2010/76/EC amending annex V, 11, 23 (a) of the Directive 2006/48/EC.

[23] Article 5, §1 of the Regulation (EC) No 852/2004 of the European Parliament and of the Council of 29 April 2004 on the hygiene of foodstuffs, *OJ L* No 226 of 25 June 2004, p. 3.

[24] See for a detailed overview R. Wearing, *Cases in Corporate Governance*, London, 25-39 (Sage, 2005).

by selling short-term futures. The long-term contracts had to be closed out due to a fall in the oil prices resulting in losses of over USD 1 billion.[25] In 1995 Nick Leeson of Barings Bank bought and held unauthorized positions in future contracts instead of arbitraging the contracts. He speculated on the future increase of the Nikkei index, but inter alia due to the Kobe earthquake of 1995 the Japanese stock index waned. Barings Bank lost USD 1.3 billion and was declared bankrupt.[26]

3. New Risk Management Duties

The first years of the new millennium experienced a number of large debacles and the legislators all around the world were encouraged to take further action. The most famous of them all was Enron. Enron made use of special purpose vehicles and moved debt off its balance sheet but things went wrong. It had to reduce shareholders' equity by USD 1.2 billion and take more than USD 0.5 billion after-tax charges before restating its earnings for four years. Its stock price collapsed from USD 90 to less than USD 1.[27] The collapse of Enron was accompanied with the failure of Global Crossing misrepresenting its financial condition and inflating its revenues. At Worldcom the internal control department discovered fraudulent revenues and capitalization of expenses.[28] In Europe similar fraudulent activities were discovered in large companies among the continents. Since the 1970s Parmalat carried an aggressive expansion policy and saw its debts rising. In 2003 the company's accounts proved the company being cash rich while it experienced significant difficulties to make EUR 150 million bond payment. It was discovered that EUR 3.9 billion of the company's funds which should be held in a Bank of America's account in name of a subsidiary did not exist. Deloitte and Grand Thornton were the auditors, but their audits failed to discover the fraudulent activities.[29] Also Vivendi engaged in an aggressive take-over policy and paid significant

[25] See for a detailed overview John Digenan, Dan Felson, Robert Kelly and Ann Wiemert, *Metallgesellschaft AG: A Case Study*, http://prmia.org/pdf/Case_Studies/MG_IIT.pdf (accessed 31 January 2013).
[26] See for a detailed overview Eric Benhamou, *Barings bank (risk management disaster)*, http://www.ericbenhamou.net/documents/Encyclo/Barings%20bank.pdf (accessed 31 January 2013).
[27] See for a detailed overview J. Solomon, *Corporate Governance and Accountability*, Chicester, 28-39 (Wiley, 2010).
[28] See for a detailed overview R. Wearing, *Cases in Corporate Governance*, London, 83-94 (Sage, 2005).
[29] See for a brief analysis J. McCahery and E. Vermeulen, *Corporate Governance Crises and Related Party Transactions: A Post-Parmalat Agenda*, in *Changes of Governance in*

amounts of goodwill. When the dotcom bubble burst, Vivendi experienced significant financial difficulties and accumulated losses of more than EUR 30 billion. A new CEO could rescue the company and rebuild Vivendi in a healthy company.[30] Shell overestimated its oil reserves, Eurotunnel was largely underestimating developing costs and overestimating revenues, Lernout&Hauspie (L&H) established 'independent' subsidiaries which had to pay royalties to L&H financed through loans to the company, etc.

While many different reasons formed the basis of the financial difficulties and collapses of many large companies, a common problem was the insufficient monitoring structures and the perception of failed internal controls. Legislators and regulators were called upon.

### 3.1.European Risk Management

Both at the European level as well as at national levels the board of directors was asked to pay more attention to risk management. Trust needed to be restored with adequate controls to mitigate the accidents that happened. The 2004 Transparency Directive requires that issuers' annual and interim reports include 'a description of the principal risks and uncertainties that [it] face[s]' and 'The interim management report shall include at least an indication of important events that have occurred during the first six months of the financial year, and their impact on the condensed set of financial statements, together with a description of the principal risks and uncertainties for the remaining six months of the financial year'.[31] The requirement to disclose the principal risks and uncertainties obliges companies to install at least a risk and uncertainty identification system. In a proposal for the modernization of this directive ESMA is empowered to issue guidelines with respect to these disclosure requirements.[32] The identification of risks was already required in the prospectus to be published when the company is stock exchange listed. The requirements can be found in the

---

*Europe, Japan and US*, K.J. Hopt et.al (Ed.), Oxford, 225-228 (Oxford University Press, 2005).

[30] G. Johnson, K. Scholes, R. Whittington, F. Fréry, *Etude de cas: Vivendi Universal à la conquête de la convergence médiatique*, http://www.strategique8.pearson.fr/libre/ressources/historique/chap01/chap01_cas_vivendi.pdf (accessed 1 February 2013).

[31] Article 4, § 2, subpart c and article 5, § 4 Directive 2004/109/EG of the European Parliament and the Council of 15 December 2004 on the harmonization of transparency requirements with regard to information about issuers whose securities are admitted to trading on a regulated market, *OJ* L No 390 of 31 December 2004, p. 38.

[32] Proposal for a Directive of the European Parliament and of the Council amending Directive 2004/109/EC on the harmonization of transparency requirements in relation to information about issuers whose securities are admitted to trading on a regulated market and Commission Directive 2007/14/EC, COM(2011) 683 final, 25 October 2011, p. 16.

Prospectus Directive 2003/71/EC and Commission Regulation 809/2004, which oblige companies to include risk factors in the prospectus. 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. Directive 2010/73/EU further clarified what information is considered 'key information' in assessing risks related to the company and the securities:

> [ …] essential and appropriately structured information which is to be provided to investors with a view to enabling them to understand the nature and the risks of the issuer, guarantor and the securities that are being offered to them or admitted to trading on a regulated market and, without prejudice to Article 5(2)(b), to decide which offers of securities to consider further. In light of the offer and securities concerned, the key information shall include the following elements:
>
> (i) a short description of the risks associated with and essential characteristics of the issuer and any guarantor, including the assets, liabilities and financial position;
>
> (ii) a short description of the risk associated with and essential characteristics of the investment in the relevant security, including any rights attaching to the securities; [ …].[33]

Listed companies must also provide for an annual corporate governance statement according to the Directive 2006/46/EC amending the Fourth and Seventh Company Law Directives. 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'.[34] On the consolidated level, 'a 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.[35] The statement can be integrated in the management report or be published as a separate report. 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. The auditor's obligations related to the internal control and risk

[33] Article 1, §2. (a) (ii) of Directive 2010/73/EU of the European Parliament and of the Council of 24 November 2010 amending Directives 2003/71/EC on the prospectus to be published when securities are offered to the public or admitted to trading and 2004/109/EC on the harmonization of transparency requirements in relation to information about issuers whose securities are admitted to trading on a regulated market, *OJ* L No 329 of 11 December 2010, p. 1.

[34] Article 1, §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 No 224 of 16 August 2006, p. 1.

[35] Article 2, §2, Directive 2006/46/EC.

management system is limited to the financial reporting process, like the American requirements in SOX. Many of the aforementioned malpractices were either directly or indirectly related to financial 'tricks' for which an adequate internal control system, controlled by an external expert, could be seen as an appropriate answer.

The external auditor has to control the availability in the corporate governance statement on the description of the main features of the system in relation to the financial reporting process and issue an audit 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.[36]

Next to the disclosure requirements in the Transparency and Accounting Directives, the Directive 2006/43/EC 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.[37] This obligation goes beyond the disclosure requirements of the Transparency Directive and the amendments of the Accounting Directives and covers one of the components of an enterprise risk management system. The monitoring requirement, i.e. monitoring the financial reporting process as well as the internal control system, significantly increases the responsibility of the audit committee. According to Article 41 of Directive 2006/43/EC the audit committee must not only monitor the effectiveness of the internal control system of financial reporting, but the effectiveness of all internal control, internal audit and risk management systems. It can be derived from this duty that the company must install such systems allowing the audit committee to monitor their effectiveness but the Directive does not provide any guidance as to which kind of system is appropriate. The audit committee will have to collect information about all the different components and procedures of the applied systems and assess the functioning of the systems for which criteria need to be developed. The criteria allows the committee to assess if the systems provide for reasonable assurance that the goals can be reached.

[36] FEE, *Discussion Paper for Auditor's Role Regarding Providing Assurance on Corporate Governance Statements*, 36 (Brussels, 2009).

[37] Article 41, § 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.

In 2005 the European Commission issued a recommendation on independent directors and committees of the board which contains additional guidelines structuring the audit committees' work.[38] In fact, the recommendation is broader than the scope of the Directive 2006/43/EC on statutory audits. The recommendation contains several principles related to the role of the audit committee. This committee should assist the board in its task to, e.g. :

- 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 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. [39]

Both Directive 2006/43/EC on statutory audits and the 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 Directive 2006/43/EC 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 only has to assess the effectiveness of the internal audit function and external audit process.[40]

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

[38] 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.
[39] *Ibid.*, Annex I, Committees of the (supervisory) board, p. 61.
[40] The latter duty being further limited to specific subtasks, namely the responsiveness of the management and the functioning of the head of internal audit.

financial reporting process'.[41] The role of the auditor vis-à-vis the internal control process is limited. The European auditor must report the material weaknesses but has no monitoring duty regarding the effectiveness control of the audit committee. According to Directive 2006/43/EC monitoring the effectiveness of the system in relation to financial reporting remains the sole duty of the audit committee. In the US, management must provide an assessment of the effectiveness of internal control for financial reporting.

In the recitals of Directive 2006/43/EC, the collective responsibility of the board is stressed. Article 41, paragraph 2 of Directive 2006/43/EC also emphasizes the responsibility of the board members. It stresses the delicate borderline between the audit committee's responsibilities and the board of director's responsibility. According to Directive 2006/43/EC the audit committee's duties go beyond the mere advisory work to prepare the board meetings. The committee has four monitoring duties and one reviewing task.[42] The audit committee should inform the board of directors about the work program allowing the board to monitor the work of the committee.

### 3.2. National Risk Management Provisions

Next to the European rules[43] some national Member States introduced, often since the start of the corporate governance era, legislative and regulatory requirements related to internal control and risk management. These obligations can be divided into three groups: (i) substantive provisions, (ii) disclosure requirements and (iii) (comply or explain) best practices. Substantive provisions and disclosure requirements are mandatory and provided in the national companies' acts or codes. An alternative is the incorporation of the rules in the binding listing requirements of a stock exchange. Companies issuing their shares on a (regulated) market must comply with these listing rules. Best practices can either add guidance to the substantive provisions or to the disclosure requirements.

#### 3.2.1. Substantive Provisions

[41] Article 41, § 4, Directive 2006/43/EC.

[42] Monitoring the financial reporting process; monitoring the effectiveness of the company's internal control, internal audit where applicable, and risk management systems; monitoring the statutory audit of the annual and consolidated accounts; reviewing and monitoring the independence of the statutory auditor or audit firm, and in particular the provision of additional services to the audited entity (Article 41, § 2, Directive 2006/43/EC).

[43] The transposition of these European Directive provisions will not be further discussed.

Substantive provisions on risk management and internal control are few. In 1998 the German Parliament enacted the Control and Transparency in Business Act (KonTraG) under which it was provided that the management board must 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[44], can impair the net worth, financial position and results of the company in a sustainable manner, are 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.[45]

In 2010 the Danish Companies act was modernized, and it is provided that the board of directors, or in case the company has opted for a two-tier board structure, the supervisory board, must ensure that 'adequate risk management and internal control procedures have been established'. The Danish law does not provide any additional guidance to companies as to what is considered an 'adequate' system. The Danish corporate governance code which was amended in 2011 to integrate the new Companies Act only recommends an annual identification of the most important business risks as well as communication between the executive and the supervisory boards of the most important areas of risk and compliance including the adopted policies, frameworks etc. in order to enable the supervisory board to assess the development and make the necessary decisions.[46] The Danish act also provides indirectly for a similar early risk recognition system as the German act.[47]

The UK Companies Act 2006 requires the director to consider inter alia the likely consequences of any decision in the long term and the impact of the company's operations on the community and the environment[48]. However, boards of listed companies must comply

[44] K. Schmidt and M. Lutter, *Aktiengesetz Kommentar,* Köln, 1035-1036 (O. Schmidt Verlag, 2008).
[45] § 317 (4) Handelsgesetzbuch.
[46] Danish Committee on Corporate Governance, *Recommendations on Corporate Governance*, recommendations 8.1.1 and 8.1.2, 2011, p. 19.
[47] The board of directors or the supervisory board is responsible for ensuring that 'the financial resources of the limited liability company are adequate at all times, and that the company has sufficient liquidity to meet its current and future liabilities as they fall due. The limited liability company is therefore required to continuously assess its financial position and ensure that the existing capital resources are adequate.' (Article 115, § 5 andarticle 116, § 5 of the Danish Companies Act).
[48] Section 172 (a) and (d) of the UK Companies Act 2006.

with more stringent internal control provisions. The UK Listing Rules compel companies to apply the Main Principles of the UK Corporate Governance Code and report to shareholders on how they have done so.[49] Main principle C 2 makes the board 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'. The Financial Reporting Council's Internal Control Guidance for Directors on the Combined Code provides in details what it considers a 'sound' system.

> 'An internal control system encompasses the policies, processes, tasks, behaviours and other aspects of a company that, taken together:
> - facilitate its 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;
> - help ensure the quality of internal and external reporting. […];
> - help ensure compliance with applicable laws and regulations, and also with internal policies with respect to the conduct of business.
> A company's system of internal control will reflect its control environment which encompasses its organizational structure. The system will include:
> - control activities;
> - information and communication processes; and
> - processes for monitoring the continuing effectiveness of the system of internal control.
> The system of internal control should:
> - be embedded in the operations of the company and form part of its culture; […].[50]

Other countries only indirectly force the establishment of an internal control or risk management system. France is an example of this approach. The French Commercial Code requires the board of directors to perform all controls and verifications that it considers expedient.[51]

---

[49] FSA, *FSA Handbook Listing, Prospectus and Disclosure*, LR 9.8.6 (5).
[50] FRC, *Internal Control Guidance for Directors on the Combined Code*, 2005, http://www.frc.org.uk/Our-Work/Publications/Corporate-Governance/Turnbull-guidance-October-2005.aspx (accessed 1 February 2012).
[51] Article 225-35, section 3, the French Commercial Code.

### 3.2.2. Disclosure Requirements

More common than the substantive risk management provisions are the internal control/risk management disclosure requirements. Although binding, transparency offers companies more leeway as to the implementation of the duty providing in internal control and/or risk management. The European Union compels the disclosure of 'the principal risks and uncertainties' and 'the main features of the company's internal control and risk management systems in relation to the financial reporting process'.

Since 2003 the chairman of the board of directors of a French listed company or, in case the company is organized with a two-tier board 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.[52] 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. As the law does not provide any additional guidelines, the supervisory authority Autorité des Marchés Financiers (AMF) first referred to the guidelines of the employers' associations AFEP-MEDEF[53] to satisfy in these reporting provisions. However, The AMF noticed that companies were insufficiently informed of the range of these disclosure requirements and 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. 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 second year assessed the adequacy of the internal control procedures in place. [54] To overcome this problem the AMF installed a commission, the Groupe de Place, to develop an internal control guide. This committee had to take into account the COSO framework as well as the pending proposals for European Directives regarding internal control. COSO is a well-known framework of internal control and enterprise risk management. According to

[52] Article L 225-37 and 225-68, the French Commercial Code.

[53] AMF, *Gouvernement d'entreprise et contrôle interne: obligations de publication des émetteurs faisant appel public à l'épargne*, 1 Revue mensuelle de l'Autorité des Marchés Financiers, 39-41 (Mars, 2004).

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

COSO, a risk management framework should help companies in achieving their strategic, operations, reporting and compliance objectives.[55] For COSO the role of the board of directors is pivotal. The board of directors must play a critical role in 'overseeing an enterprise-wide approach to risk management' which includes 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.[56] In its report the Groupe de Place clearly distinguishes (reporting) between 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.[57] The requirements are aligned but not identical with 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. The French Commercial Code requires the chairman not only to report on the internal control procedures but also on risk management. Hence, The French framework identifies more objectives which resemble the 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. In 2010 the Groupe the Place report[58] was updated inter alia to integrate the new European requirements to have the audit committee involved in the effectiveness process.[59]

While the French disclosure requirements of risk management are intended to provide shareholders and investors with valuable information, the Dutch legislator improved the communication between the management board and the supervisory board in 2004. In particular, the legislator aimed at improving the reporting between the two boards in non-listed companies.[60] At least once a year the management board must notify the supervisory

[55] Committee of Sponsoring Organizations of the Treadway Commission, *Enterprise Risk Management – Integrated Framework*, Executive Summary, AICPA Inc., 3 (New York, 2004).

[56] Committee of Sponsoring Organizations of the Treadway Commission, *Effective Enterprise Risk Oversight: The Role of the Board of Directors*, AICPA Inc. p. 2-3 (New York, 2009).

[57] Groupe de Place, *Le dispositif de Contrôle Interne: Cadre de référence*, 65 p. (Paris, January 2007).

[58] The report explicitly mentions: 'Ultimately, it is a tool that should ensure greater uniformity of the concepts underpinning the drafting of chairmen's reports on internal control and risk management and the work of audit committees.' (AMF, *Risk management and internal control systems*, 4 (Paris, 2010)).

[59] AMF, *Risk management and internal control systems*, 42, (Paris, 2010).

[60] Dutch Parliament (Chamber), *Explanatory memorandum to the change of book 2 of the civil code related to the amendments of the structured regime*, nr. 28179/ 3, p. 27 (2001–2002).

board of the principles on the strategic policy, the general and financial risks and the management and control of the company.[61] The aim was to improve the effectiveness of the monitoring duties of the supervisory board.

### 3.2.3. Comply or Explain Best Practices

In many jurisdictions a balanced approach between mandatory requirements and best practices related to risk management has been utilized. The best practices are both used to further clarify or add provisions to the substantive legal framework or to help the companies to fulfill their transparency obligations vis-à-vis the supervisory board, the shareholders or the investors.

#### 3.2.3.1. Refining and Completing the Legislative Provisions

In the UK, next to the aforementioned mandatory main principle C 2 to maintain sound internal control and the risk management system, the UK Corporate Governance Code foresees in an additional risk management code provision C.2.1. that 'the board should, at least annually, conduct a review of the effectiveness of the company's risk management and internal control systems and should report to shareholders that they have done so. The review should cover all material controls, including financial, operational and compliance controls'.

In the Dutch Corporate Governance Code a number of provisions regards risk management and internal control, both at the level of the organization of the system as well as at the level of reporting to the shareholders and the investors. These duties are added to the yearly risk disclosure requirements of the management board to the supervisory board.[62] As a general principle, the Code identifies as management duties 'the strategy and associated risk profile, the development of results and corporate social responsibility issues that are relevant to the enterprise'[63]. Besides, the management board is responsible 'for complying with all relevant primary and secondary legislation, for managing the risks associated with the company

[61] Book 2: 141, § 2 Dutch Civil Code (introduced by Law 9 July 2004, *Dutch OJ* No 370).
[62] See above 3.2.2.
[63] Monitoring Committee, *Dutch Corporate Governance Code*, Principle II.1 (2008).

activities and for financing the company'[64]. The Code offers the management board in further guidance as to the content of a risk management system in best practice provision II.1.3.:

> The company shall 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 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.

Next it stresses the monitoring duties of the supervisory board which must include '[…] b) corporate strategy and the risks inherent in the business activities; c) the design and effectiveness of the internal risk management and control systems; d) the financial reporting process; e) compliance with primary and secondary legislation […]'[65] The explanatory notes to the Code add that the suitability requirements provide more leeway for smaller companies.[66] Additional guidance as to the content of the code of conduct and the guides is lacking.

The Belgian Companies Act does not provide for specific risk management requirements other than those that follow from the European Directives.[67] The Belgian corporate governance code adds that it is the board's responsibility to 'decide on the company's values and strategy, its risk appetite and key policies'[68]. The overall risk management framework must be prepared by the executive management, approved by the board and reviewed first by the audit committee and next by the board.[69] In provision 6.5. the code identifies what an internal control system is composed of: identification, assessing, managing and monitoring by management of 'financial and other risks without prejudice to the board's monitoring role,

---

[64] Ibid.
[65] Monitoring Committee, *Dutch Corporate Governance Code*, Provision III.1.6 (2008).
[66] Monitoring Committee, *Dutch Corporate Governance Code*, the 'Explanation of and notes to certain terms used in the code', p. 39 (2008).
[67] An analysis of the monitoring role of the board of directors related to risk management can be found in S. De Geyter, *De toezichtstaak van de raad van bestuur*, Tijdschrift voor Privaatrecht, 1175-1221 (2012).
[68] Belgian Corporate Governance Commission, *Belgian Code on Corporate Governance*, Provision 1.2 (2009).
[69] *Ibid*., provision 1.3.

based on the framework approved by the board'[70]. The code advises the chairman of the board to ensure that the induction program for new directors includes the fundamentals of the corporate risk management and internal control systems.[71] For audit committee members the program must cover a presumably more detailed 'overview' of the company's internal control organization and risk management systems.[72]

The scope of the French corporate governance code regarding internal control and risk management is limited. It comes as no surprise in light of the extensive legal disclosure requirements for which additional and extensive guidance is provided in a separate document.[73] However, the code adds one specific feature to the commercial code requirements. A French listed company must be equipped with 'reliable procedures for the identification and assessment of its commitments and risks'[74]. In particular the company must identify and monitor the 'off-balance-sheet-commitments, and [to] evaluate the corporation's material risks'.[75]

The Danish corporate governance code was amended in 2011 to align it with the new companies act. The Danish Act requires the board to establish risk management and internal control procedures. The Code falls short in guiding the companies as to which procedures comply with this mandatory requirement.[76] The Code only recommends to yearly identify the most important business risks 'associated with the realization of the company's strategy and overall goals as well as the risks associated with financial reporting'[77]. The aforementioned COSO enterprise risk management framework[78] goes well beyond risk identification.

[70] *Ibid*., provision 6.5.
[71] *Ibid*., guideline to provision 4.8.
[72] *Ibid*., guideline to provision 4.9.
[73] See above 3.2.2.
[74] AFEP-MEDEF, *Corporate Governance Code of Listed Corporations*, Recommendation 2.2, p. 8 (2010).
[75] *Ibid*. p. 9.
[76] See above 3.2.1.
[77] Danish Committee on Corporate Governance, *Recommendations on Corporate Governance*, Recommendation 8.1.1, p. 19 (2011).
[78] See above 3.2.2

3.2.3.2. Disclosure Best Practices

Many corporate governance codes recommend informing the shareholders and/or the supervisory board on risk management and internal control related issues. Disclosing risk management related topics can decrease the information asymmetries between the incumbent parties and the outsiders of the company and provide the latter with valuable information for monitoring the company and assessing their investments.

The Dutch corporate governance code clarifies article 141, Book 2, Civil Code with the notification requirement of the supervisory board of inter alia the general and financial risks. According to provision III. 1.8. the management board must discuss with the supervisory board 'the corporate strategy and the main risks of the business, the result of the assessment by the management board of the design and effectiveness of the internal risk management and control systems, as well as any significant changes thereto', the result of which must be presented in the annual report of the supervisory board.

Next the Dutch code introduced the 'corporate governance statement' in 2003. Originally, the statement had to declare that (all) systems are adequate and effective, the 2008 edition softened it to the declaration that the system provides reasonable assurance that the financial reporting process contains no errors of material importance. Next to this 'declaration' the management board must 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.[79] The system set out by the COSO reports is considered appropriate.

The Danish Recommendations on Corporate Governance contains similar transparency provisions as the Dutch code, although less extensive and detailed. Provision 8.1.2 recommends the management board to report to the supervisory board 'on the development within the most important areas of risk and compliance with adopted policies, frameworks

[79] Monitoring Committee, *Dutch Corporate Governance Code*, Provision II.1.4 (2008).

etc. in order to enable the supreme governing body to track the development and make the necessary decisions'. The annual report should contain information about the business risks[80] next to the European requirements but no 'statement' like in the Netherlands. It is likely that the limited disclosure recommendations are due to the very general relevant Danish legal and regulatory requirements. Both the Danish law and the code require risk management and internal control procedures but fail to provide for any guidance as to the substantive requirements.[81]

The UK Corporate Governance Code adds to the content of the corporate governance statement[82] in the annual report the reasons, if applicable, why no internal audit function has been in place and the reasons, if applicable, why the board has taken a different position vis-à-vis the audit committee's recommendation on the appointment, reappointment or removal of an external auditor.[83]

4. European National Case Law

The developments of the board's duties related to internal control and risk management raise the question how courts in many jurisdictions read and apply the new mandatory and regulatory requirements. Aforementioned we referred to the famous American cases *Smith v. van Gorkum*, *Re Caremark*, *Stone v. Ritter* and *Citigroup* of which the latter in particular illustrates that the decision-making process must be sound, and the court should not take into account whether the decision is 'right or wrong'. American case law was already well established when new legislative risk management requirements were enacted. In Europe the picture is more blurred and there are a number of cases that seem to indicate that the requirements of appropriately addressing risk (management) and engaging in risky business are not always properly distinguished.

The requirement of monitoring, including the evolution of operational risks is well established in many jurisdictions. In the Barings case the court of appeal upheld the court's decision of director's disqualification because the director failed to ensure that the 'activities were

[80] Danish Committee on Corporate Governance, *Recommendations on Corporate Governance*, Recommendation 8.3.1, p. 19 (2011).
[81] See above 3.2.1 and 3.2.3.1.
[82] FSA, *FSA Handbook Listing*, *Corporate Governance Statements*, DTR 7.2.1.
[83] FRC, *UK Corporate Governance Code*, p. 30 (September 2012).

properly monitored and/or controlled'. In particular, the director 'failed to pay any or any sufficient regard to […] the lack of any proper system by which to monitor and control […] risk limits, the lack of any proper assessment of […] compliance with risk limits or reported profitability against those risk limits, the absence of a risk and compliance officer'[84]. The monitoring duty must be performed with reasonable care and skill but it is not 'considered that those responsibilities can go so far as to require the non-executive directors to overrule the specialist directors, like the finance director, in their specialist fields. The duty is not to ensure that the company gets everything right. The duty is to exercise reasonable care and skill up to the standard which the law expects of a director of the sort of company concerned, and also up to the standard capable of being achieved by the particular director concerned'[85].

The monitoring duties are company-specific and even strategy-specific. In the Netherlands the Enterprise Chamber decided that in the light of the very ambitious goals and a business plan that did not provide for any control moments so that execution time could be adjusted, and if necessary be stopped, the supervisory board had to control meticulously the developments of the company. It could also have been expected that the supervisory board would have demanded that a contingency plan had been prepared.[86]

A number of cases withheld the liability of the (supervisory) board when one particular risk management component is violated. As part of the internal environment, the board of directors must decide how much risk is acceptable in pursuing the corporate objectives, the risk appetite. COSO defines the risk appetite as 'the amount of risk, on a broad level, an organization is willing to accept in pursuit of value'[87]. In some cases the courts consider the risk appetite of the company unacceptable and the (supervisory) board is held liable. In the ARAG/Garmenbeck case the German Bundesgerichtshof decided that the management board can be held liable when the boundaries of responsible behavior, exclusively based on a corporate welfare creating activity and on a careful investigation, is in an irresponsible way

---

[84] *Re Barings plc and others (No 5), Secretary of State for Trade and Industry v. Baker and others (No 5)*, 1 BCLC 286 (1999).

[85] *Re Continental Assurance Co of London plc (in Liquidation) (No 4)*, 2 BCLC 287 (2007); All ER (D) 229 (2001) (also, *Singer v. Beckett*); quoted on http://www.purnells.co.uk/limited-company/dont-do-this/law-library/wrongful-trading-law.html (accessed 5 February 2013). For a short analysis of the case see T. Bachner, *Wrongful trading before the English High Court: Re Continental Assurance Company of London plc (Singer v. Beckett)*, EBOR, 195-200 (2004).

[86] *Laurus*, Ondernemingskamer Gerechtshof Amsterdam, 16 October 2003, 174/2003, LJN:AM 1450, http://zoeken.rechtspraak.nl **(**accessed 5 February 2013).

[87] COSO, *Enterprise Risk Management: Understanding and Communicating Risk Appetite*, p. 1 (January 2012).

breached or if the behavior of the board for any other reason is regarded wrongful.[88] Later the Oberlandesgericht Düsseldorf decided in the IKB case that no board is careful when it takes business risks, which, if realized, lead to the downfall of the company.[89] Similar cases can be found in the Netherlands. In Laurus the Enterprise Chamber concluded that the Board of Directors takes irresponsible risks if, notwithstanding negative signals, it supports the continuation of the business plan even when it endangers the survival of the company. […]. There is no rational justification not to seriously test the adequacy of the project.[90] Closely related to this case is the decision of the Court of Utrecht that found both the board and the supervisory board liable because they have opted for a strategy without any assessment of the thereto related risks.[91] The Court of Appeal of Mons (Belgium) found the board of directors liable for the bankruptcy of the company because there was not an appropriate risk management system in accordance with the size and operational activities of the company.[92]

Another component for which the (supervisory) board has been held liable is an insufficient information and communication system. The Enterprise Chamber considered the supervisory board liable because the board should not have relied merely on information from the management but had to request a(nother) thorough analysis […], inter alia through the use of external consultants in order to find other solutions than the sole reliance on bank financing.[93]

While the cases that have been discussed are well motivated and seem to indicate that the courts diligently proceed, some, like the Laurus case, illustrate that the courts will have increasing difficulties to judge without hindsight bias. The new legal and regulatory risk management requirements aggravate this hindsight bias risk. There are already some signs of increased accountability of directors for having business risk *mitigating* systems instead of risk *management* systems. In a recent Belgian case one director was convicted for the corporate breaching of the environmental legislation.[94] The company fell short of compliance

[88] *ARAG/Garmenbeck*, Bundesgerichtshof 21 April 1997, AG 1997, 377; BGHZ 135, 244; NJW 1997, 1926; ZIP 1997, 883.
[89] IKB, Oberlandsgericht Düsseldorf 9 December 2009, AG 2010, 126.
[90] *Laurus*, Ondernemingskamer Gerechtshof Amsterdam, 16 October 2003, 174/2003, LJN:AM 1450, http://zoeken.rechtspraak.nl **(**accessed 5 February 2013).
[91] *Ceteco*, Rechtbank Utrecht 12 December 2007, 171413/ HA ZA 04-34, LJN: BB9709 http://zoeken.rechtspraak.nl (accessed 5 February 2013).
[92] Court of Appeal Bergen 3 March 2008, *RRD* 2008, 295-296.
[93] *KPNQuest*, Ondernemingskamer Gerechtshof Amsterdam 28 December 2006, 1301/2005, LJN: AZ5413, http://zoeken.rechtspraak.nl (accessed 5 February 2013).
[94] Court of Appeal Gent, 25 November 2011, *TRV* 2012, 711, 734, comment S. De Geyter.

with the environmental legislation related to water sanitation. The board of directors systematically underinvested in the exploitation of the plant and priority was given to economize instead of complying with new environmental laws. The individual board member should have protested against this underinvestment which implies that board members must ensure that a system that identifies and mitigates regulatory (environmental) risks is in place. Although it consists of a criminal case, Belgian board members must object against (at least certain kinds of) risky activities and make sure that risk management systems identify these significant risks.

Generally, the new risk management system requirements are open standards which leave many options to manage the risks. If a risk is not identified or an identified risk is materializing, the system is not necessarily flawed. Different systems identify different kinds of risks and provide for different responses to manage the risks. One need to be almost supernatural in distinguishing ex post risks for which directors must be accountable and other risks. The next section advocates for a European, more balanced alternative.

## 5. Assessing the European (Member States) Models of Board Responsibility for Risk Management

Since the turn of the millennium we have experienced a proliferation of risk management related rulemaking. Board of directors and management must be aware that running the corporation requires more risk management compliance than in the previous decades. The board must make sure that its monitoring duty is embedded in a reasonably designed risk management and internal control (reporting) framework. However, the components that are provided in the legislative frameworks in many European Member States are still developing. COSO defined enterprise risk management as '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'.[95] The entity objectives are divided into four categories: strategic,

[95] Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Enterprise Risk Management – Integrated Framework*, Executive Summary, p. 2. (COSO II Report) (AICPA, 2004). Internal control is 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, and compliance with applicable laws and regulations" (Committee of Sponsoring Organizations of the Treadway Commission (COSO), Internal Control – Integrated Framework, Executive Summary, p. 2. (COSO I Report) (AICPA, 1992).

operations, reporting and compliance.[96] Most legislative and regulatory framework do not address all components of the risk management framework, nor do they refer to all objectives that the company according to the COSO framework must identify. The main findings of the analysis are summarized in table 1.

Table 1: Summarized Overview of ERM Requirements in different Member States

| | ERM system/ ERM component | objective | specified | substantive/ disclosure | instrument | "Hard" law Comply/Explain Best practice |
|---|---|---|---|---|---|---|
| European Union | risk identification | all | no* | disclosure | Directive | Hard law |
| | monitor (effectiv.) | all | no | substantive | Directive | Hard law |
| | system | financial reporting | no | disclosure | Directive | Comply/Explain |
| | control | all | partially | substantive | Recommendation | best practice |
| | internal audit (effectiv.) | all | partially | substantive | Recommendation | best practice |
| | external audit (effectiv. | all | partially | substantive | Recommendation | best practice |
| Belgium | system | all | yes | substantive | Code | Comply/Explain |
| Denmark | system | all | no | substantive | Law | Hard law |
| | risk identification | all | no | substantive | Code | Comply/Explain |
| | risk identification | strategy/fin. rep. | no | substantive | Code | Comply/Explain |
| | system | all | no | disclosure *** | Code | Comply/Explain |
| | risk identification | operations | no | disclosure | Code | Comply/Explain |
| France | system | all | no | disclosure | Law | hard law |
| | risk identif./assess. | all | no | substantive | Code | Comply/Explain |
| Germany | risk identification | all | yes (all) | substantive | Law | Hard law |
| The Nether-lands | risk identification | all | no | disclosure *** | Law | Hard law |
| | system | all | yes | substantive | Code | Comply/Explain |
| | system | all | partially | disclosure | Code | Comply/Explain |
| | internal environment | all | no | substantive | Code | Comply/Explain |
| UK | risk assessment | all | no | substantive | Law | Hard law |
| | risk identification | all | no | substantive | Code | Comply/Explain** |

[96] Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Enterprise Risk Management – Integrated Framework*, Executive Summary, p. 3. (COSO II Report) (AICPA, 2004).

| | | | | | |
|---|---|---|---|---|---|
| system | all | yes | substantive | Code | Comply/Explain |
| monitor (effectiv.) | all | yes | disclosure | Code | Comply/Explain |
| monitor (internal audit) | all | yes | disclosure | Code | Comply/Explain |

*: the prospectus directive provides further guidance; **: main principle must be applied; ***: towards the supervisory board

Many components of the risk management system must, according to both the legislator and the regulator, cover all objectives while guidance as to the soundness of the system is often lacking. Risk management is relatively new and best practices in the field are still evolving making the implementation of effective risk management systems a challenging board's task.[97] Obviously many companies struggle with the risk management regulations. The Dutch Monitoring Commission Corporate Governance qualitatively assessed the monitoring performance of the supervisory board and found that a large majority of the boards complies with the requirement to monitor the risks related to the business activities and the design and effectiveness of the internal risk management and control systems (Table 2). However, the results also show that a significant number of companies just pass the minimum requirements, or even do not pass the test. Next, more supervisory boards monitor the strategy and risks than the risk management system.

Table 2: Monitoring of the Supervision of (Dutch provision III.I.6):

| | Strategy and risks | Internal risk management and control systems |
|---|---|---|
| no reporting | 3% | 8% |
| Technically complies with the provision | 40% | 61% |
| Complies with the recommendations regarding providing insight into the activities performed and focus areas | 35% | 22% |
| Complies more than the recommendations require by also providing a subjective rating such as a vision. | 22% | 9% |

Source: based on Monitoring Commission Corporate Governance Code, *Fourth report on compliance with the Dutch Corporate Governance Code*, December 2012, Table 15, p. 32.

[97] S. Bainbridge, *Corporate Governance after the Financial Crisis*, Oxford, p. 173 (Oxford University Press, 2012). The state of the art of the board's monitoring role can be found in Protiviti, *Board Risk Oversight: A Progress Report*, www.protiviti.com, 16 p. (December 2010) (accessed 31 July 2011).

Companies that are confronted with the materialization of a significant risk and which are in the midst of developing and improving an evolving risk management system, and companies that have taken a sound business decision to implement a limited[98] risk management framework, can fear liability claims for the inadequacy of the system.Courts will have to apply rules visualized in table 1 that go beyond the sound business judgment. It can be questioned whether an effective risk management system which can at best prevent a number of risks from materializing or limit the impact of the risks that do materialize is sufficient to meet the expectations of legislators and regulators. This risk is unacceptable in the business decision process. Business decisions should be taken with due care, but they will always be uncertain as to the outcome. Eisenberg showed that a high liability standard will result in too much risk-averse decision making:

> It is often in the interests of shareholders that directors or officers choose the riskier of two alternative decisions, because the expected value of a more risky decision may be greater than the expected value of the less risky decision. Suppose that Corporation C has USD 100 million in assets. C's board must choose between Decision X and Decision Y. Each decision requires an investment of USD 1 million. Decision X has a 75% likelihood of succeeding. If the decision succeeds, C will gain USD 2 million. If it fails, C will lose its USD 1 million investment. Decision Y has a 90% chance of succeeding. If the decision succeeds, C will gain USD 1 million. If it fails, C will recover its investment. It is in the interest of C's shareholders that the board makes Decision X, even though it is riskier, because the expected value of Decision X is USD 1.25 million (75% of USD 2 million, minus 25% of USD 1 million) while the expected value of Decision Y is only USD 900,000 (90% of USD fc1 million). If, however, the board was concerned about liability for

[98] The development of a full risk management process is an intensive task. According to AIRMIC, Alarm and IRM, this policy must include (AIRMIC, Alarm, IRM, *Structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000*, p. 10, http://theirm.org/documents/SARM_FINAL.pdf, (2010) (accessed 5 February 2013): Risk management and internal control objectives (governance); Statement of the attitude of the organization to risk (risk strategy); Description of the risk aware culture or control environment; Level and nature of risk that is acceptable (risk appetite); Risk management organization and arrangements (risk architecture); Details of procedures for risk recognition and ranking (risk assessment); List of documentation for analyzing and reporting risk (risk protocols); Risk mitigation requirements and control mechanisms (risk response); Allocation of risk management roles and responsibilities; Risk management training topics and priorities; Criteria for monitoring and benchmarking of risks; Allocation of appropriate resources to risk management; Risk activities and risk priorities for the coming year.

> breaching the duty of care, it might choose Decision Y, because as a practical matter it is almost impossible for a plaintiff to win a duty-of-care action on the theory that a board should have taken greater risks than it did. A standard of review that imposed liability on a director or officer for unreasonable as opposed to irrational decisions might therefore have the perverse incentive effect of discouraging bold but desirable decisions. Putting this more generally, under an ordinary standard of care directors might tend to be unduly risk-averse, because if a highly risky decision had a positive outcome, the corporation but not the directors would gain, whereas if it had a negative outcome, the directors might be required to make up the corporate loss.[99]

A recent strategy dilemma of the two major Swiss banks, UBS and Credit Suisse, illustrates that the example of Eisenberg is not inconceivable. UBS addresses the difficult financial era with higher capital requirements and low returns with 'winding down large parts of its risky fixed income trading'[100]. Credit Suisse has chosen the opposite path. According to one analyst there is more upside for Credit Suisse in the short run but more stability for UBS in the long run. It is clear that both strategies have pros and cons, and it is unpredictable which is preferable or 'better'.

The same goes for the business decision related to the soundness of the applied risk management appetite and tolerance as an example of Miller illustrates:

> Properly functioning risk management systems do not eliminate risk and do not eliminate the possibility of losses, even catastrophic losses. At best, they measure risk and assist the firm in taking on the level of risk it desires. Imagine a financial firm with capital of about $100 billion using a VAR model […]. Its board of directors decides that a tolerable daily risk level is a $100 million VAR with 99 per cent confidence. Even if all the assumptions on which such models are based are correct – in particular that the historical pattern of covariances of risk factors will continue into the future – this means that the firm is taking a 1 per cent chance every day of losing more than $100 million.

[99] M. Eisenberg, *The Divergence of Standards of Conduct and Standards of Review in Corporate Law*, Fordham Law Review, 444-445 (1993).
[100] J. Schotter and D. Schäfer, *Big Swiss lenders bank on opposing strategies*, Financial Times, p. 15 (4 February 2013).

> Put another way, every three to four months, the firm can expect to have a trading day in which its losses exceed $100 million. Large financial firms also use VAR models to calculate their annual risk of bankruptcy. For example, such a firm might accept a 0.5 per cent annual chance of a loss sufficient to bankrupt the company. Thus, the bank is accepting the risk that it should expect to go bankrupt once in two hundred years. If the bank happens to suffer such a loss this year, that is no proof that its risk management systems were at fault. Consequently, the materialization of risks and consequent losses prove nothing about supposed deficiencies in risk management.[101]

Rule-based models are insufficient to mitigate or manage these risks as the result would inevitably reduce the undertaking risky ventures. Managing strategy should not be confused with managing risks. Therefore we would like to advise further developing the legislative risk management programs in distinguishing the risk management requirements between the strategic and operational objectives on the one hand and compliance and financial reporting objectives on the other hand. For the former the board of directors must define the risk appetite of the company and systematically consider the categories of risks that can occur and monitor the processes to manage these risks. A business judgment rule is an appropriate instrument to assess whether – in case a strategic and/or operational risk materializes – the board of directors should have assessed and responded to it. The system can only work if the duty of loyalty of directors is strengthened. The CEO of Worldcom continued with a failing operational risk management because the management's self-interest contributed to it. It could be that he resisted to effective operation risk management because it would have affected his compensation scheme.[102]

The situation is different for compliance and financial reporting objectives. Regulatory and legal compliance programs including product quality, labor protection, financial reporting, etc., are tools to identify and mitigate these risks. Many of these risks are preventable or manageable if appropriate monitoring processes are installed and the effectiveness of the processes is regularly tested. For these types of risk, risk management resembles legal compliance programs and they should be fully developed under the monitoring role of the board of directors.

---

[101] R. Miller, *Oversight Liability for Risk Management Failures at Financial Firms*, Southern California Law Review, 94-95 (2010).

[102] S. Bainbridge, *Corporate Governance after the Financial Crisis*, Oxford, p. 172-173 (Oxford University Press, 2012).

In its recent communication, the European Commission emphasizes the importance of risk disclosure. The communication is vague as to the approach to reach this goal but it stresses that the means are an 'effective design' to address those risks providing in a comprehensive risk profile.[103] The aforementioned distinction can fit into this approach and is also compatible with the mandatory framework of the accounting directive. However, it will be insufficiently for improving the equilibrium between entrepreneurship and risk control as the regulatory framework is too fragmented and insufficiently distinguishes between the business risk management approach and the reporting and the compliance risk approach.

[103] European Commission, *Communication-Action Plan: European company law and corporate governance - a modern legal framework for more engaged shareholders and sustainable companies*, COM(2012) 740 final, p. 6 (12 December 2012).

# Financial Law Institute

The **Financial Law Institute** is a research and teaching unit within the Law School of the University of Ghent, Belgium. The research activities undertaken within the Institute focus on various issues of company and financial law, including private and public law of banking, capital markets regulation, company law and corporate governance.

The **Working Paper Series**, launched in 1999, aims at promoting the dissemination of the research output of the Financial Law Institute's researchers to the broader academic community. The use and further distribution of the Working Papers is allowed for scientific purposes only. Working papers are published in their original language (Dutch, French, English or German) and are provisional.



More information about the Financial Law Institute and a full list of working papers are available at:
**http://www.law.UGent.be/fli**