Risk Management in European and American Corporate Law

Law Working Paper N°.122/2009
April 2009

Christoph Van der Elst
Tilburg University, Ghent University and ECGI

Marijn van Daelen
Tilburg University

ECGI Working Paper Series in Law

Risk Management in European and American Corporate Law

Working Paper N°.122/2009

April 2009

Christoph Van der Elst
Marijn van Daelen

Abstract

In recent years, the emphasis in corporate governance has shifted from board composition, independent directors, separating the position of chairperson and CEO, and establishing board committees to "being in control" and risk management issues. However, the corporate law perspective of internal control and risks management does not match up to the multidisciplinary perspective of these themes. This paper analyses the dichotomy between the US and the EU corporate law approaches to internal control and risk management. Lawmakers from the US, the EU, and the EU member states reacted to the scandals between 2000 and 2003 with provisions requiring public companies to have internal control and risk management systems in order to restore public confidence, but the substance of their responses differed. A regulatory framework is put forward in order to address the steps to be taken in establishing an operational internal control and risk management framework and to address the role of the different parties involved from a corporate law perspective. The abovementioned steps are: (1) initiate and identify, (2) assess and operate, (3) monitor, and (4) report on the systems relating to the companies' risks and uncertainties, strategy, financial reporting, and operations. The parties legally involved include: (1) senior management, (2) board, (3) audit committee, and (4) auditor. The US and the EU regulatory frameworks indicate not only that their corporate law approaches to internal control and risk management are different, but also that both approaches are incomplete – but not necessarily insufficient – in several areas.

Keywords: risk management, corporate law, internal control, COSO, SOX, corporate governance, EU corporate law

JEL Classifications: G32, K22, G30, M42

Christoph Van der Elst
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

Marijn van Daelen
University of Tilburg
Warandelaan 2
PO Box 90153
5000-LE Tilburg
The Netherlands
e-mail: m.m.a.vandaelen@uvt.nl

Table of contents

1. Introduction

"With regards to controls, Siemens is in a position where it cannot afford to fail again. But how could we monitor 10 million, in peak times even 40 million transactions a day?"[1] "Two reports into what went wrong with SocGen's internal controls painted a damning picture of weak procedures, poor implementation and bad management."[2] These quotations refer to the difficulties of internal control of large companies. In the case of Siemens, the 2006 scandal over allegations of bribery highlighted its corporate governance shortcomings, with CFO Kaeser facing the need to redesign the compliance system and reshape the corporate audit system. In 2008, the ongoing issue of monitoring internal control lead to the purchase of a €60m computer system aimed at tracking down violations of internal control. In the case of SocGen, there were management and risk control failures. Although SocGen acknowledged these failures, even with well-functioning internal control and risk management systems, fraudulent behaviour could slip through the cracks due to a lack of proper oversight.

These two examples are taken from a long list of articles that illustrate the shift in corporate governance emphasis from board composition, independent directors, separating the position of chairperson and CEO, and establishing board committees to the issue of "being in control", resulting in utterances such as "I want to get a director jailed" in the special Financial Times report on digital business.[3] In the report, it was also argued that adequate procurement and management processes including software audits must be in place. Because of the emphasis on the internal control aspect of corporate governance over the last years, internal control and risk management provisions are now more sophisticated than ever before.

This paper will first discuss internal control and risk management from an organisational, accounting, and economic perspective (section 2). The company law framework does not directly match up to this multidisciplinary perspective on control, as section 3 will show. At first sight, the important role of management, as distinct from the role of the board of directors, seems neglected in corporate law as all relevant general powers are in the hands of the board of directors. In sections 4 and 5, the US and EU approaches to internal control and

[1] Daniel Schäfer, *The champion of a new culture of control*, Financial Times, 1 October 2008.

[2] Hal Weitzman, *Hunt is stepped up for the rogue traders*, Financial Times, 20 October 2008.

[3] Financial Times, *Special Report - FT Digital Business*, 28 February 2007, p. 1.

risk management will be analysed. The US, the EU, and the EU member states reacted to the scandals with provisions requiring public companies to have internal control and risk management systems in order to restore public confidence, but the substance of their responses differed. Section 6 shows an analysis of this dichotomy in approach. Section 7 provides the concluding remarks.

2. A multidisciplinary view of internal control and risk management

Control has long been seen as an essential and central process of management. In his seminal work *General and Industrial Management*,[4] Henri Fayol, a mine engineer and, according to some, the father of operational management theory, wrote that the five functions of management are planning, organizing, commanding, coordinating, and controling.[5] Control is a cornerstone of management as it ensures that the activities of the organisation are in line with the planned results.

From an organisational perspective, control is defined as "a process whereby management or other groups are able to initiate and regulate the conduct of activities such that their result accord with the goals and expectations held by those groups."[6] In this light, control is considered to be more than just a system for transmit information to support the initiation and regulation of the organisation's endeavours. It aims to ensure that a predictable level and type of outcome are attained and maintained, e.g., the process of control.

Accounting literature studies financial reporting and internal and external control procedures for enhancing financial reporting reliability. The external auditor serves as the gatekeeper of financial information. Internal control refers to accounting controls and measures in organizations which protect the assets and information of the company and to related credibility tests.[7] The external auditor's review should provide a fair assessment of the financial statements: can these statements reasonably be considered reliable and do they not mislead investors as to the condition of the internal control? Generally, internal control

[4] Originally published in 1917 as *Administration industrielle et générale.*

[5] In recent literature, "commanding" and "coordinating" have been merged into "leading".

[6] J. Child, *Organization: Contemporary Principles and Practice*, Oxford: Blackwell Publishing, 2005, p. 112.

[7] S. Maijoor, "The Internal Control Explosion", *International Journal of Auditing*, 2000:4, pp. 104-105.

provides reasonable assurance that the entity's objectives will be met. Among other things, these internal control systems provide responsiveness to corporate risks. However, for a long time internal control only served as support for the external audit since control was seen as the "general system upon which the books have been kept".[8] The accounting view of control is related to the economic analysis of control that is dominated by the agency theory. It focuses on the mitigation of costs due to the separation of ownership and control and expropriation of the majority shareholder vis-à-vis the minority shareholders.

The debate on the importance of adequate internal control systems to *manage* companies actively started to be emphasized at the end of the last century. In 1985, due to a number of scandals and failures, the US National Commission on Fraudulent Financial Reporting (the Treadway Commission) was established. The Commission's objective was to identify and respond to the risk of fraudulent reporting. Many of the Commission's recommendations emphasized the importance of sufficient internal controls. In 1992, the Treadway Commission issued the report *Internal Control – Integrated Framework* (COSO I) and defined internal control 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."[9]

The Treadway Commission later broadened its scope and shifted its focus towards risk management. In 2004, the Commission released its report *Enterprise Risk Management – Integrated Framework* (COSO II) to take internal control to the next level and include effective risk management. Risk management is "the process whereby organisations methodically address the risks attaching to their activities with the goal of achieving sustained

[8] L. Dicksee, *Auditing: A Practical Manual for Auditors*, London: Gee and Company, 1892. Reprinted Arno Press, New York 1976, p. 8.

[9] Committee of Sponsoring Organisations (Treadway Commission), Internal Control – Integrated Framework (COSO I report), *Executive Summary*, 1992, p. 1. COSO was formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting.

benefit within each activity and across the portfolio of all activities".[10] The COSO II report identified four different categories for the achievement of an entity's objectives:[11]

"- Strategic: high-level goals, aligned with and supporting its mission
- Operations: effective and efficient use of its resources
- Reporting: reliability of reporting
- Compliance: compliance with applicable laws and regulations."

One effect of this report is that the internal control system is generally seen as a part of the broader risk management system. Risk is often defined as the probability of an undesirable event or as the variability of future outcomes, whereas before, it was seen as an adverse event that could only be overcome ex post. Risk is closely related to uncertainty and exposure. Uncertainty is commonly used to describe a state of not knowing whether a proposition is true or false, but the degree of uncertainty does not affect the degree of exposure to that proposition.[12] Risks are identifiable and measurable whereas uncertainties are identifiable but not measurable.[13] Another group of events are the unknowable events that are not identifiable let alone measurable. However carefully companies plan for contingencies, the number and range of threats that confront them are overwhelming: terrorism risks, investment risks, e-commerce risks, liability risks, weather risks, political risks, credit risks, etc. Risk management strives to enable management to effectively deal with identifiable events that can have an adverse effect on the company.[14]

---

[10] IRM (The Institute of Risk Management) & AIRMIC (The Association of Insurance and Risk Managers) & ALARM (The National Forum for Risk Management in the Public Sector), *A Risk Management Standard*, 2002.

[11] Committee of Sponsoring Organisations (Treadway Commission), Enterprise Risk Management – Integrated Framework (COSO II report), *Executive Summary*, 2004, p. 3.

[12] G. A. Holton, "Defining risk", *Financial Analyst Journal*, CFA Institute, Volume 60, No. 6, 2004, pp. 21-22.

[13] F. H. Knight, *Risk, Uncertainty, and Profit*, Boston, MA: Hart, Schaffner & Marx; Houghton Mifflin Company, 1921, Chapter I, p. 26: "It will appear that a *measurable* uncertainty, or "risk" proper, as we shall use the term, is so far different from an *unmeasurable* one that it is not in effect an uncertainty at all. We shall accordingly restrict the term "uncertainty" to cases of the non-quantitive type." See also J. M. Keynes, *A Treatise on Probability*, London: Macmillan, 1921; F. P. Ramsey, "Truth and Probability", *The Foundations of Mathematics and Other Logical Essays*, New York: Harcourt Brace, 1931; and L. J. Savage, *The Foundations of Statistics*, New York: John Wiley & Sons, 1954.

[14] See also the reference in the COSO II report (p. 1) to uncertainty as "present[ing] both risk and opportunity, with the potential to erode or enhance value. Enterprise risk management enables management to effectively deal with uncertainty and associated risk and opportunity, enhancing the capacity to build value."

This enterprise risk management framework, including the internal control system, must be embedded in an appropriate corporate environment. In its 1992 report, the Treadway Commission identified five key components, which are necessary to achieve the corporate objectives, some of which are closely related to essential corporate governance features: the control environment, risk assessment, control activities, information and communication, and monitoring. In its 2004 enterprise risk management system, the Commission added three additional components: objective setting, event identification, and risk response. As the title of the report indicates, the new components illustrate the increased emphasis on risk and risk behaviour.

The control environment concerns the operating style of the board of directors. Risk assessment refers to the identification and qualitative and quantitative analysis of relevant risks, especially their likelihood and expected impact. Control activities are the procedures and processes that help ensure that the entity guidelines are carried out. Information and communication ensure the dissemination of the necessary information throughout the organisation with respect to internal control and risk management, including the top-down and the bottom-up approach. Monitoring relates to the review of and the follow up to internal control, which is an ongoing process to assess and maintain the quality of the system. Objective setting is defining the risk appetite and tolerance of the organisation. Event identification is the recognition of incidents that affect – negatively as well as positively – the achievement of objectives. Risk response relates to the identification and assessment of the responses to risk, depending on the risk appetite of the organisation.

Several components, such as the control environment and monitoring, require the commitment of those in charge of corporate governance. By contrast, an effective and efficient internal control system involves all personnel of an organisation. Following the COSO II report, the board of directors provides governance and monitoring and has an important role vis-à-vis the control environment. The audit committee plays an important role in monitoring the effectiveness of the internal control framework. Management must ensure the development, implementation, and improvement of the framework as well as its effectiveness. Management sets the objectives and aligns the objectives with the company's mission given its risk appetite. Next, the events that can affect the achievement of the objectives must be identified while distinguishing between threats and opportunities.

Management must select the risk responses in accordance with the company's risk appetite: avoiding, accepting, reducing, or sharing risk. Internal audit assists management with this process. The implementation and application of the internal control framework are, to some degree, all other personnel's responsibility. Finally, the COSO II report sets out that the external auditor controls the effectiveness and reliability of internal control over – at least – financial reporting. However, the COSO II report does not align the duties of the parties involved with the legal framework of responsibility and liability. These issues will be addressed in the next section.

In short, an effective internal control system requires an effectively communicated and implemented – hence monitored – framework allowing the corporate constituents to take appropriate decisions. Compliance with internal control requirements requires the company to develop a framework via which the risk management cycle is implemented. The cycle involves the identification of risks and uncertainties, the analysis of implications, the response to mitigate or accept risks, and the allocation of appropriate contingencies,[15] as well as an adequate reporting and monitoring system.

3. A corporate law view of internal control and risk management

The company law framework does not directly match up to this multidisciplinary perspective of control. At first sight, the important role of management, as distinct from the role of the board of directors, seems neglected in corporate law as all relevant general powers are in the hands of the board of directors. The US statutory model states that the board of directors runs the company: "All corporate powers shall be exercised by or under the authority of the board of directors of the corporation, and the business and affairs of the corporation shall be managed by or under the direction, and subject to the oversight, of its board of directors."[16] The UK model articles of association for public companies[17] provide that the directors (a)

[15] Smith, N., *Engineering Project Management*, Oxford: Blackwell Science, 1995.

[16] Section 8.01(b) of the Model Business Corporation Act 2005. See also the Delaware Code that provides that the corporation's business and affairs "shall be managed by or under the direction of a board of directors."

[17] As amended in 2007. See Regulation 70 of Table A of the Commencement 1 October 2007, Companies (Tables A to F) Regulations 1985 as Amended by SI 2007/2541 and SI 2007/2826. The Companies Act 2006 received Royal Assent on 8 November 2006 and the provisions must be implemented by October 2009. The Act

shall manage the company's business; and (b) may exercise all the powers of the company for any purpose connected with the company's business.

However, an important qualification must be introduced. Almost all boards use their authority to delegate. Operational decisions and day-to-day management of the company are delegated to senior management and subordinate employees. In the US Corporate Director's Guidebook, it is stated:[18]

> It is generally recognized that the board of directors is not expected to operate the business. Even under statutes providing that the business and affaires shall be "managed" by the board of directors, it is recognized that actual operation is a function of management. The responsibility of the board is limited to overseeing such operation [….]
>
> It is important to emphasize that the role of the director is to monitor, in an environment of loyal but independent oversight, the conduct of the business and affairs of the corporation in behalf of those who invest in the corporation.

Section 3.02 of the American Law Institute's Corporate Governance Recommendations requires the board of directors to oversee the conduct of the corporation's business to evaluate whether the business is being properly managed. The New Jersey Supreme Court stated it in another way: "Directorial management does not require a detailed inspection of day-to-day management, but rather a general monitoring of corporate affairs and policies."[19]

Delegation of board authority is also recognised by the UK model articles of association for public companies:[20] "The directors may, by power of attorney or otherwise, appoint any

---

replaced existing company legislation by rewriting, updating, and modernising company law. The Companies Act 2006 provides for a new form of model articles of association for companies incorporated in the United Kingdom.

[18] Corporate Director's Guidebook of the Committee on Corporate Laws as referred to in American Law Institute, *Principles of Corporate Governance: Analysis and Recommendations*, St. Paul, 1992, Comment on §3.01, p. 83.

[19] New Jersey Supreme Court, *Francis v. United Jersey Bank*, 87 N.J. 15, 432 A.2d 814, 1981.

[20] Regulation 71 of Table A of the Commencement 1 October 2007, Companies (Tables A to F) Regulations 1985 as Amended by SI 2007/2541 and SI 2007/2826.

person to be the agent of the company for such purposes and on such conditions as they determine, including authority for the agent to delegate all or any of his powers." The articles continue:[21]

> The directors may delegate any of their powers to any committee consisting of one or more directors. They may also delegate to any managing director or any director holding any other executive office such of their powers as they consider desirable to be exercised by him. Any such delegation may be made subject to any conditions the directors may impose, and either collaterally with or to the exclusion of their own powers and may be revoked or altered. Subject to any such conditions, the proceedings of a committee with two or more members shall be governed by the articles regulating the proceedings of directors so far as they are capable of applying.

Management directs operations; the board of directors retains the power to hire and fire management and employees, and to monitor and discipline management. This kind of oversight function is not performed by actively supervising senior management but by evaluating its performance, that of the CEO in particular, and dismissing underperforming managers.

Policymaking remains an important task of the board of directors and it is involved in the decisions affecting the future development of the corporation.[22] In some jurisdictions, this function is explicitly assigned to the board of directors. For example, Article 524bis of the Belgian Companies Act requires the board of directors to set the general policy of the company in case a separate executive committee (*directiecomité*) is established.

Monitoring management is both a supportive and a watchful process and includes the supervision of the conduct of the corporation's business. It comprises the control over the development of appropriate compliance programs, the circulation of these programs to

[21] Regulation 72 of Table A of the Commencement 1 October 2007, Companies (Tables A to F) Regulations 1985 as Amended by SI 2007/2541 and SI 2007/2826.

[22] K. Andrews, "Rigid Rules Will Not Make Good Boards", *Harvard Business Review*, Nov.-Dec. 1982, No. 35, p. 44.

employees, and procedures for the maintenance of the programs.[23] While it is mandatory for the board to monitor the business, corporate law fails to address the questions of *how* a board of directors can comply with the duty of oversight and *which systems* must be applied to reach the goal of oversight compliance. These issues will be addressed in the next section.

4. The US approach to internal control and risk management

After a number of high-profile scandals between 2000 and 2003 in the US, Europe, and Australia, internal control became one the most challenging issues for companies, especially for those charged with implementing good governance. The focus was mainly on internal control systems for financial reporting and risk management systems. Companies needed to restore public confidence, and risk management and internal control systems offer a framework to respond to market concerns and to reflect a sound business practice. Many countries issued requirements, and these requirements vary considerably in detail and prescriptiveness. The best-known is the 2002 US federal regulation for public companies, the Sarbanes-Oxley Act (SOX). It requires the CEO and the CFO to report on and certify the effectiveness of the company's internal control over financial reporting. However, this requirement is not the only internal control requirement US companies have to comply with.

4.1 From an accounting-based approach towards a corporate and securities-based approach to internal control

The securities reform after the market crash in the autumn of 1929 emphasized for the first time the importance of internal control. Regulation S-X required the external auditor to consider the "adequacy of the system of internal check and internal control. Due weight might be given to an internal system of audit regularly maintained by means of auditors employed on the registrant's own staff".[24] External auditors were allowed to rely on the system

[23] American Law Institute, *Principles of Corporate Governance: Analysis and Recommendations*, St. Paul, 1992, Comment on §3.01, p. 89.

[24] Heier, Dr. Jan R., Dugan, Michael T., and Sayers, David L., "Sarbanes-Oxley and the Culmination of Internal Control Development: A Study of Reactive Evolution". American Accounting Association, 2004, *Mid-Atlantic Region Meeting Paper*, p. 3. (Available at SSRN: http://ssrn.com/abstract=488783.)

implemented by the corporation, if they consider that system to be appropriate. Weaknesses in the system affected the scope of the audit and required additional controls. Hence, the system only served the audit and had a limited scope.

This US audit-oriented approach changed in 1977 after a number of corporate scandals related to the bribery of foreign officials.[25] In accordance with the 1977 Foreign Corrupt Practices Act (FCPA), the US Securities and Exchange Commission (SEC) requires reporting companies to keep books, records, and accounts and to maintain internal control reviews in order to control management activities. The relevant section reads:[26]

> Every issuer which has a class of securities registered [...] and every issuer which is required to file reports [...] shall [...] devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that:
> i. transactions are executed in accordance with management's general or specific authorization;
> ii. transactions are recorded as necessary to permit preparation of financial statements in conformity with generally accepted accounting principles or any other criteria applicable to such statements, and to maintain accountability for assets.

Companies are allowed to choose the framework they consider fit to comply with the FCPA requirements. In case of non-compliance with the FCPA, corporate violators face criminal and civil liability claims. The SEC can investigate companies that issue financial instruments and bring civil injunction actions against them to the Department of Justice for prosecution. Penalties are subject to the US Sentencing Commission's guidelines. These guidelines became effective for organisations in 1991. An important feature of the guidelines is the sentencing credit. Effective corporate programs that prevent and detect violations of law can help

[25] Companies named include Lockheed, Bendix, and IT&T; see A. Reinstein and A. Spalding, "The Audit Committee's Role Regarding the Provisions of the Foreign Corrupt Practices Act", *Journal of Business Strategy*, 1995, No. 12, pp. 23-35.

[26] 15 U.S.C. section 78m (b) (2) (B).

mitigate potential fines.[27] Under the 1994 guidelines, the effectiveness of such programs was evaluated against seven criteria:[28]

- Establishment of compliance standards;
- Oversight by high-level personnel;
- Due Care in delegating substantial discretionary authority;
- Effective Communication to all levels of employees;
- Reasonable steps to achieve compliance, which include systems for monitoring, auditing, and reporting suspected wrongdoing without fear of reprisal;
- Consistent enforcement of compliance standards including disciplinary mechanisms;
- Reasonable steps to respond to and prevent further similar offenses upon detection of a violation.

The sentencing credit would only be provided if the organisation fully cooperates and includes the disclosure of all pertinent information known by the organisation.

Ex post court decisions further provided helpful insights on the management of appropriate internal control systems. In the *Caremark* decision,[29] Chancellor W. T. Allen expanded the traditional view of the directors' duty to exercise oversight by writing:[30]

> 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,

[27] Fine ranges are based on the seriousness of the offense and the culpability.

[28] U.S. Sentencing guidelines manual § 8A1.2, comment 3(k) (1 November 1994), and see: P. Desio, *An Overview of the Organisational Guidelines*, to be downloaded free of charge at http://www.ussc.gov/orgguide.htm, 2004. In May 2004, Section 8A1.2(b)(2)(D) was amended by adding at the end "To determine whether the organization had an effective compliance and ethics program for purposes of §8C2.5(f), apply §8B2.1 (Effective Compliance and Ethics Program)", and the commentary to §8A1.2 was amended by striking note 3(k).

[29] See *In re Caremark Int'l Derivative Litig.*, 698 A.2d 959 (Del. Ch. 1996).

[30] Ibid., p. 5. Before the *Caremark* decision, the rule for the duty of corporate directors was given in *Graham v. Allis-Chalmers Manufacturing Co* (188 A.2d 125, 130 (Del. 1963)), where the court concluded that "absent cause for suspicion there is no duty upon the directors to install and operate a corporate system of espironage to ferret out wrongdoing which they have no reason to suspect exists."

render a director liable for losses caused by non-compliance with applicable legal standards.

He also noted that the potential sentence could be reduced under the Federal Sentencing Guidelines if the company had a compliance program.

In addition to criminalising corporate conduct, securities regulation started to emphasize the importance of adequate disclosure of management's risk assessments. In 1982, Item 303 on Management's Discussion and Analysis of Financial Condition and Results of Operations (MD&A) was added to Regulation S-K. The SEC had adopted the present form of the disclosure requirements for MD&A as early as 1980.[31] The management report must report on the material events and uncertainties that can cause financial information to be less indicative of future results and condition. Hence, these reporting requirements compel management to assess all risks and threats companies may encounter and to address the issues in a reliable management's discussion and analysis statement. "The discussion and analysis shall focus specifically on material events and uncertainties known to management that would cause reported financial information not to be necessarily indicative of future operating results or of future financial condition."[32] In particular, management must address uncertainties and events that can influence liquidity, capital resources, results of operations, off-balance sheet arrangements, and especially contractual relationships.[33]

---

[31] See <http://www.sec.gov/rules/interp/33-8350.htm>.

[32] Title 17 (Commodity and Securities Exchanges), Part 229 (Regulation S-K), Item 303 ("Management's discussion and analysis of financial condition and results of operations") of the Code of Federal Regulations, § 229.303; see "Instructions to paragraph 303(a)", under no. 3. The cited reporting requirement existed before SOX was developed (see 17CFR229.303, Code of Federal Regulations, Title 17, Volume 2, Revised as of April 1, 2002, From the U.S. Government Printing Office via GPO Access), and it did not change after the enactment of SOX (see 47 FR 11401, Mar. 16, 1982, as amended at 47 FR 29839, July 9, 1982; 47 FR 54768, Dec. 6, 1982; 52 FR 30919, Aug. 18, 1987; 68 FR 5999, Feb. 5, 2003; 73 FR 958, Jan. 4, 2008).

[33] The MD&A rules (see § 229.303) require disclosure of (among other things):

- Information necessary to an understanding of the registrant's financial condition, changes in financial condition and results of operations;
- Any known trends, demands, commitments, events or uncertainties that will result in, or that are reasonably likely to result in, the registrant's liquidity increasing or decreasing in any material way;
- The registrant's internal and external sources of liquidity, and any material unused sources of liquid assets;

Notwithstanding this shift of the legislation from an *accounting-based* approach towards a *corporate and securities-based* approach to internal control, issues related to internal control were almost exclusively tackled in accounting principles and literature. The Treadway Commission was established and started its preparatory work on the COSO report, and the Auditing Standards Board issued nine new standards to address the expectation gaps in auditing: the 1988 Statement on Auditing Standards No. 55,[34] which required auditors to assess the internal control structure in a financial statement audit.

4.2 Changing the scene: SOX requirements

Corporate scandals changed the aforementioned accounting approach considerably. In response to the US failures of Enron, WorldCom, and Andersen, Congress passed the 2002 SOX, a major shift in US securities and corporate regulation. SOX had to restore faith and trust in the reliability of the financial information provided by companies. It contains substantive corporate governance mandates and not just disclosure requirements.[35] SOX

- The registrant's material commitments for capital expenditures as of the end of the latest fiscal period;
- Any known material trends, favorable or unfavorable, in the registrant's capital resources, including any expected material changes in the mix and relative cost of capital resources, considering changes between debt, equity and any off-balance sheet financing arrangements.
- Any unusual or infrequent events or transactions or any significant economic changes that materially affected the amount of reported income from continuing operations and, in each case, the extent to which income was so affected.
- Significant components of revenues or expenses that should, in the company's judgment, be described in order to understand the registrant's results of operations;
- Known trends or uncertainties that have had, or that the registrant reasonably expects will have, a material favorable or unfavorable impact on net sales or revenues or income from continuing operations.
- Matters that will have an impact on future operations and have not had an impact in the past.

[34] Auditing Standards Board, Statement on Auditing Standards (SAS) No. 55: *Consideration of the Internal Control Structure in a Financial Statement Audit*, April 1988. The Auditing Standards Board (ASB) is the senior technical committee of the AICPA designated to issue auditing, attestation, and quality control standards and guidance.

[35] R. Romano, *The Sarbanes-Oxley Act and the Making of Quack Corporate Governance*, Yale ICF Working Paper No. 05-23, September 2005, 1.

covers such specific substantive topics as: independence of accountants, independent oversight over the work of independent accountants, audit committee composition, internal control provisions, granting loans to executives, and provisions relating to financial analysts. However, SOX also contains provisions enhancing disclosure by companies, in combination with these substantive provisions. The compliance methods, including structural implications, for the disclosure requirements are left to the company. The most prominent provision, Section 404, relates to the maintenance, evaluation and effectiveness of the internal control of financial reporting. Its prominence eclipses other provisions, such as reporting on off-balance sheet transactions, filing beneficial ownership, the disclosure of the code of ethics for senior financial officers, and even the other certification requirements.

Section 404 compels companies to establish and maintain an adequate internal control structure and procedures for financial reporting for which management is responsible. It also requires an evaluation of the effectiveness of the internal control structure and procedures for financial reporting.[36] Additionally, the auditor has a duty to control and certify the management effectiveness reports.

Compared to Section 404, Section 409 is less often discussed, but its impact should not be overlooked. It requires real-time issuer disclosures:[37]

> Each issuer reporting under section 13(a) or 15(d) shall disclose to the public on a rapid and current basis such additional information concerning material changes in the financial condition or operations of the issuer, in plain English, which may include trend and qualitative information and graphic presentations, as the Commission determines, by rule, is necessary or useful for the protection of investors and in the public interest.

Hence, Section 409 requires the implementation of *real-time* monitoring systems for the companies' financial condition or operations. Regulated companies could face organisational

[36] Section 404 a (1) and (2) SOX.

[37] Section 13 of the Securities Exchange Act of 1934 (15 U.S.C. 78m) was amended by adding this requirement at the end.

complications as they must identify operational information in a timely fashion and establish procedures for responding to that information.[38]

Besides Sections 404 and 409, SOX contains other provisions dealing with internal control for financial reporting. Section 302 requires the CEO and the CFO to provide a certification both of the fairness of the financial statements and information in each quarterly and annual report and of their responsibility for establishing and maintaining internal controls. Further, the CEO and the CFO must certify that they have evaluated the effectiveness of the internal controls and have presented in the report their conclusions about the effectiveness of their internal controls based on their evaluation.[39] Additionally, the CEO and the CFO must disclose to the auditors and the audit committee significant deficiencies and material weaknesses in the design or operation of internal control over financial reporting and any fraud that involves management or employees who significantly participate in the internal control procedures for financial reporting.[40]

Compared to Section 302, Section 404 deals with more enhanced financial disclosures. Section 302 requires the CEO and the CFO to certify their responsibility for establishing and maintaining *internal controls* and to present their conclusions about the effectiveness of the internal controls in the annual or quarterly report. By contrast, Section 404 requires the annual report to contain an internal control report that states the responsibility of management – not limited to CEO and CFO – for establishing and maintaining an *adequate internal control structure and procedures for financial reporting* and to contain an assessment – not only the conclusions – of the effectiveness of the internal control structure and procedures.

According to Section 906, the CEO and the CFO must also provide the market with a certification that "the periodic report containing the financial statements fully complies with" the requirements of Section 13(a) or 15(d) of the 1934 Securities Exchange Act "and that information contained in the periodic report fairly presents, in all material respects, the financial condition and results of operations of the issuer." Statements that do not comport with this requirement can result in a fine of up to USD 1m and/or ten years imprisonment.

[38] For a more detailed analysis of the organisational complications of SOX section 409, see: A. D. Morrison, Sarbanes Oxley, *Corporate Governance and Operational Risk*, Sarbanes-Oxford Seminar, 22 July 2004, p. 11.

[39] Section 302 a (3) and (4) SOX.

[40] Section 302 a (5) SOX.

Wilfully certifying inaccurate statements will drive the penalty up to USD 5m and/or twenty years imprisonment.

Section 301 requires that audit committees "establish procedures for [...] the receipt, retention, and treatment of complaints [...] regarding accounting, internal accounting controls, or auditing matters". In combination with Section 406, which requires the board to adopt a code of ethical conduct, it obliges companies to develop more formal mechanisms to report on and to handle internal *shortcomings* in business practice.

Section 205 (a) deals with the audit committee. It amends Section 3(a) of the 1934 Securities Exchange Act by including a definition of the audit committee, whose purpose is described as overseeing the accounting and financial reporting processes and audits of the financial statements of the company.[41]

These provisions require companies to perform formal assessments of their internal controls over financial reporting, including tests to confirm both the design and operating effectiveness of the controls, as well as including in the annual report an assessment of internal control over financial reporting. The assessment must contain several statements:[42]

> - A statement of management's responsibility for establishing and maintaining adequate internal control over financial reporting for the company.
> - A statement identifying the framework used by management to conduct the required evaluation of the effectiveness of the company's internal control over financial reporting.
> - Management's assessment of the effectiveness of the company's internal control over financial reporting as of the end of the company's most recent fiscal year, including a statement as to whether or not the company's internal control over financial reporting is effective. The assessment must include disclosure of any "material weaknesses" in the company's internal control over financial reporting identified by management. Management is not permitted to conclude that the company's internal control over

[41] See 15 U.S.C. 78c(a).

[42] The Institute of Internal Auditors, *Sarbanes-Oxley 404: A Guide for Management by Internal Controls Practitioners*, April 2006, p. 11.

financial reporting is effective if there are one or more material weaknesses in the company's internal control over financial reporting.

- A statement that the registered public accounting firm that audited the financial statements included in the annual report has issued an attestation report on management's assessment of the registrant's internal control over financial reporting.

4.3 Extending the scene

The new legal requirements forced the SEC and the Public Company Accounting Oversight Board (PCAOB) to adopt rules to implement SOX. The list of regulations that both oversight bodies have issued is long but the most important and influential documents with respect to internal control are:

- SEC final rule 33-8124 of 29 August 2002 on Certification of Disclosure in Companies' Quarterly and Annual Reports
- SEC final rule 33-8238 of 5 June 2003 on Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports
- PCAOB 2004 Auditing Standard No. 2 – An Audit of Internal Control Over Financial Reporting Performed in Conjunction with An Audit of Financial Statements.[43]

Whereas the SEC rules require management to evaluate the procedures of internal control over financial reporting and test the effectiveness, the PCAOB standard requires auditors to adhere to criteria in performing an audit of a company's internal control over financial reporting to attest to and report on management's assessment. The SEC rules do not provide specific guidance on the methods to be used for the conduct of the evaluation, nor does the SEC oblige companies to apply a specific internal control framework. However, the SEC does identify the COSO report *Internal Control – Integrated Framework* as an example of a suitable framework.[44] This framework defines the categories (1) operations (2) financial

[43] Later modified in PCAOB Auditing Standard No. 5 (cf. infra).

[44] See Section II. B. 3. a. of Final Rule 33-8238 of 5 June 2003 on Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports.

reporting, and (3) compliance with applicable laws and regulations. The definition of internal control provided by the SEC does not encompass the categories relating to the company's operations and compliance in general, but it does include compliance with applicable laws and regulations directly related to the preparation of financial statements.[45] Nonetheless, the COSO report does not contain the procedures to be applied in evaluating the effectiveness of the internal control system for financial reporting. Nor was there a market convention on what constitutes effective controls over financial reporting.[46] Hence, management had to develop these procedures itself or turn to external advisors. Audit firms in particular were eager to deliver these kinds of services as they belong to their core business. It can be questioned whether this was an anticipated effect.

SOX compels audit firms to register with the PCAOB and apply its standards. In 2004, the PCAOB issued Auditing Standard No. 2 regarding the auditor's obligation to attest to and to report on management's assessment of the effectiveness of internal control. This detailed rulebook offers auditors attestation guidelines. The PCAOB's standard has influenced the behaviour of management, as the latter wanted to avoid internal control and compliance discussions or conflicts with their auditors that could lead to a negative attestation and reputational damage to the company. The implementation of the procedures caused high compliance costs and probably more risk-adverse business behaviour.

The SOX provisions not only require regulators, such as the SEC and the PCAOB, to provide companies and accountants with additional guidance, but also to reassess the corporate framework for implementing the governance and control measurements. The 2005 Model Business Corporation Act (MBCA) requires all corporate powers to be exercised by or under the authority of the board of directors of the corporation. However, the official comments to Section 8.01 (b) state that in many corporations the operational management is delegated to executing officers and other professional managers.[47] Although MBCA section 8.01 (b)

[45] See Section II. A. 3. of Final Rule 33-8238 of 5 June 2003 on Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports.

[46] The Committee on Capital Markets Regulation, *Interim Report*, 30 November 2006, p. 116.

[47] Committee on Corporate Laws of the American Bar Association, Model Business Corporation Act 2005, Section 8.01 "Requirement for and duties of board of directors" under (b) and official comments to section 8.01 (b). This act is a general corporation statute that can be enacted by a state legislature; see p. xix of the Model Business Corporation Act Annotated (3rd edition). Twenty-nine states have adopted (most parts of) the Act as

allows the board of directors to delegate authority to exercise powers and perform functions to appropriate officers, employees, or agents of the corporation, the responsibility to oversee the exercise of that delegated authority remains with the board of directors.[48] The MBCA also sets the scope of the board's oversight responsibilities, which include:[49]

> (1) business performance and plans;
> (2) major risks to which the corporation is or may be exposed;
> (3) the performance and compensation of senior officers;
> (4) policies and practices to foster the corporation's compliance with law and ethical conduct;
> (5) preparation of the corporation's financial statements;
> (6) the effectiveness of the corporation's internal controls;
> (7) arrangements for providing adequate and timely information to directors; and
> (8) the composition of the board and its committees, taking into account the important role of independent directors.

The board's oversight responsibility for the preparation of the corporation's financial statements encompasses the corporation's compliance with the requirement to keep corporate records (MBCA section 16.01) and to provide financial statements to shareholders (MBCA section 16.20). Subsection 8.01(c)(6) expands the board's oversight responsibility to having internal controls in place in order to provide reasonable assurance regarding (1) the reliability of financial reporting, (2) the effectiveness and efficiency of operations, and (3) the

---

their general corporation statute, namely: Alabama, Arizona, Arkansas, Connecticut, Florida, Georgia, Hawaii, Idaho, Indiana, Iowa, Kentucky, Maine, Massachusetts, Mississippi, Montana, Nebraska, New Hampshire, North Carolina, Oregon, Rhode Island, South Carolina, Tennessee, Utah, Vermont, Virginia, Washington, West Virginia, Wisconsin, and Wyoming. Other jurisdictions have statutes based on the 1969 version of the Act (see Alaska, the District of Columbia, New Mexico, and South Dakota) or have only adopted selected provisions of the Act.

[48] Committee on Corporate Laws of the American Bar Association, *Model business corporation act annotated: official text with official comments and statutory cross-references*, revised through 2005, Chapter 8, p. 8-6.

[49] Section 8.01(c) of the Model Business Corporation Act 2005. This section was added to the MBCA after its 2002 revision (see Committee on Corporate Laws of the American Bar Association, Model Business Corporation Act, 3rd Edition, Official Text, revised through 2002).

compliance with applicable laws and regulations.[50] Guidance can be found in the 2004 revision of the US sentencing guidelines, which developed the effective compliance and ethics program as a separate section of the guidelines embedding the seven criteria to evaluate the effectiveness of the program to prevent and detect violations of law in a more elaborate framework.[51]

MBCA subsection (c)(7) of 8.01 provides that the board is responsible for overseeing that the corporation has information and reporting systems in place to provide its directors with appropriate information in a timely manner. As explained above, receiving information in a timely manner is crucial because SOX section 409 requires real-time monitoring, but also since subsection (c)(7) envisages that an appropriate system would permit the directors to discharge their responsibilities.[52]

MBCA section 8.31 provides the standards of liability for directors. It provides that a director is not liable, unless it is established that the challenged conduct consisted or was the result of:[53]

> a sustained failure of the director to devote attention to ongoing oversight of the business and affairs of the corporation, or a failure to devote timely attention, by making (or causing to be made) appropriate inquiry, when particular facts and circumstances of significant concern materialize that would alert a reasonably attentive director to the need therefore.

Case law provides additional guidelines and criteria for companies concerned with addressing compliance risks in relation to the aforementioned requirements. Much of the current standard of director's duty of care in the oversight and monitoring context derives from the 1996

[50] Committee on Corporate Laws of the American Bar Association, *Model business corporation act annotated: official text with official comments and statutory cross-references*, revised through 2005, Chapter 8, p. 8-6, see official comments.

[51] See U.S. Sentencing guidelines manual §8B2.1 (2004).

[52] Committee on Corporate Laws of the American Bar Association, *Model business corporation act annotated: official text with official comments and statutory cross-references*, revised through 2005, Chapter 8, p. 8-7, see official comments.

[53] Section 8.31, subsection a, under (2)(iv) MBCA.

Caremark decision discussed above.[54] In the post-SOX era, the Delaware Supreme Court affirmed the Caremark standard for the director's duty with respect to corporate compliance programs in its decision in *Stone v. Ritter* of 6 November 2006.[55]

4.4 Towards a balance in compliance costs and confidence

Parts of SOX were considered overwhelmingly burdensome. The criticism resulted in a draft principle-based standard to redirect the focus of auditors and to restore the pole position of the US securities markets. Mid-December 2006, the SEC responded to the heavy criticism of the regulatory burden that SOX places on businesses in relation to internal control.[56] The SEC proposed to soften the procedures of internal control and grant wider management discretion by allowing management to focus on the greatest risks.[57] The SEC's overhaul came soon after the publication of the interim report from the Committee on Capital Market Regulation.[58] The report assessed section 404 of the SOX, which was enacted without any extensive public scrutiny and without extensive research on what constitutes effective controls. It resulted in an open-ended standard without quantitative benchmarks and raised many questions for corporations and auditors who were trying to set the appropriate control level to comply with the legal requirements. An insufficient internal control threshold induces criminal and/or civil liability for management (and auditors). Throughout the regulatory changes dealing with internal control and risk management – in the pre-SOX *Caremark* case as well as in the post-SOX *Stone v. Ritter* case, and in the *Saito v. McCall* case – the standard for director liability for failure to monitor remained the same so that "only sustained or systematic failure of the

[54] R.F. Burch, *Director Oversight and Monitoring: The Standard of Care and the Standard of Liability Post-Enron*. Wyoming Law Review, Vol. 6, No. 2, 2006, pp. 485-490.

[55] *Stone v. Ritter*, 911 A.2d 362, 2006 Del. LEXIS 597.

[56] See Securities and Exchange Commission, 17 CFR Parts 210, 240 and 241, Management Report on Internal Control Over Financial Reporting, (Release Nos. 33-8762; 34-54976; File No. S7-24-06) RIN 3235-AJ58, 20 December 2006.

[57] The SEC adopted the proposed amendments of its December 2006 Proposing Release (see Securities and Exchange Commission, 17 CFR Parts 210, 228, 229 and 240, Amendments to Rules Regarding Management's Report on Internal Control Over Financial Reporting, (Release Nos. 33-8809; 34-55928; FR-76; File No. S7-24-06) RIN 3235-AJ58, 27 June 2007).

[58] Committee on Capital Markets Regulation, *The Competitive Position of the U.S. Public Equity Market*, December 2007, www.capmktsreg.org.

board to exercise oversight – such as an utter failure to attempt to assure a reasonable information and reporting system exists – will establish the lack of good faith that is a necessary condition to liability."[59] Nonetheless, the SOX provisions may indeed increase director liability because it sets *reasonable* standards as a minimum level for director conduct; courts may apply a stricter liability test.[60]

Besides that, evidence was found that the new US legal environment caused compliance costs that exceeded the estimated costs many times over while crowding out other (and sometimes more productive) activities. The US capital market lost part of its attractiveness as the most liquid and respected market. The figures show that the number of new initial public offerings at the London and Hong Kong stock exchanges overshadowed those at US markets.[61] Several US capital market parties pleaded for legal reforms to restore an efficient and competitive US regulatory and market environment. The aforementioned SEC initiative can be considered a first step towards an altered US legal internal control environment. Still, there are signs that the negative developments in the US markets continue.[62]

Whether a number of regulatory changes brought about these improvements cannot yet be empirically determined. However, it can be argued that the regulatory improvements were necessary to restore corporate confidence in the acceptability of the regulatory burdens on the US markets. An important step towards mitigating part of the problems is the modernisation of PCAOB Auditing Standard No. 5 that deals with an integrated audit of internal control over financial reporting in connection with financial statements.[63] Auditors must integrate the testing of controls on both the effectiveness of the internal control procedures and the audit of

---

[59] *Saito v. McCall*, No. 17132-NC, 2004 WL 3029876, (Del. Ch. Dec. 20, 2004).

[60] R.F. Burch, *Director Oversight and Monitoring: The Standard of Care and the Standard of Liability Post-Enron*. Wyoming Law Review, Vol. 6, No. 2, 2006, p. 528.

[61] See, for an overwhelming overview of data related to this issue, Committee on Capital Markets Regulation, *The Competitive Position of the U.S. Public Equity Market*, December 2007, www.capmktsreg.org. However, there is evidence that the economic impact of SOX on foreign listings was only significant for smaller companies (see J. Piotroski and S. Srinivasan, "Regulation and bonding: The Sarbanes-Oxley Act and the Flow of International Listings", *Journal of Accounting Research*, 2008, vol. 46, No. 2, pp. 383-425).

[62] See the website of the Committee on Capital Markets Regulation: http://www.capmktsreg.org/competitiveness/index.html.

[63] PCAOB, Auditing Standard No. 5, *An Audit of Internal Control Over Financial Reporting That Is Integrated with An Audit of Financial Statements*, 12 June 2007.

the financial statements. The Auditing Standard also allows auditors to choose between issuing a combined report or two separate reports. In addition, the PCAOB and the SEC aligned their diverging approaches relating to management's internal control report – laying down management responsibility for the internal control structure and procedures for financial reporting and the assessment of the effectiveness of the internal control procedures for financial reporting – and the auditor's report on the management disclosures on the management effectiveness report. It highlights the willingness of regulators to adopt a process-oriented approach to internal control procedures.

In short, the US approach combines mandatory rules regarding risk management behaviour with an obligation to inform the public regarding the effectiveness of the internal control systems. Whilst the SOX requirements stress the importance of an internally controlled financial reporting system, other legislation, in particular the sentencing guidelines and the MBCA have a wider scope. The sentencing guidelines provide relative assurance for investors as well as companies of what can be considered appropriate – i.e. liability avoiding – behaviour and the MBCA (among other things) provides the scope of board oversight responsibilities.

It remains to be seen whether this approach will be sufficient. The current credit crisis emphasizes the importance of internal control and risk management systems for the financial industry. For several months, the Financial Times splashed headlines such as "Greed was not the problem – it was poor risk management".[64] However, for many years companies have needed to have sound risk management systems in place. Before changing the regulatory framework, the debate should elaborate on whether it was the US legal internal control and risk management environment or the high complexity of the financial products involved that was the main feature causing the credit crunch. As discussed above, internal control and risk management provisions need to strike a balance between criticism that compliance costs are too high and the need to deal with a lack of investor confidence.

[64] J. Ascher, *Greed was not the problem – it was poor risk management*, Financial Times, 26 September 2008. This article states that: "What failed Wall Street and the commercial banks was their credit and market risk management systems".

5. The EU approach to internal control and risk management

Like the US, the EU and its member states responded to the major failures around the turn of the century in order to restore public confidence, but unlike the US rule-based approach, the European style was more principle-based. Also, while the US system mainly concentrates on internal control over financial reporting[65] and – as evidenced by the sentencing guidelines – fraud, the provisions adopted by the EU and its member states on internal control systems more strikingly deal with provisions additional to financial reporting.

Different European countries have developed or updated internal control requirements, in particular in their national corporate governance codes, as a reaction to the corporate failures. More recently, the EU in a number of directives and recommendations has issued a variety of rules that directly or indirectly influence the internal control organisation of listed companies. It is generally argued that the European principle-based approach offers more flexibility for companies to develop their internal control environment and avoids one-size-fits-all solutions. European member states allow the taking into account of the unique aspects of each business and the shunning of bureaucratic costs that exceed the benefits. However, the principles of internal control in the EU legislation have a much broader scope than the US SOX requirements that emphasize the effectiveness of internal control over financial reporting.[66] In particular, the new *eighth* company law directive and a European Commission recommendation require audit committees not only to assess the effectiveness of financial reporting systems but also to annually review internal control and risk management systems and ensure the effectiveness of the internal audit function in all its facets.

[65] See for example, SOX Sections 404 and 302.

[66] Nevertheless, the MBCA gives the scope of the board's *oversight* responsibilities, which includes attention to the effectiveness of the corporation's internal controls in order to provide reasonable assurance regarding (1) the reliability of *financial reporting*, (2) the effectiveness and efficiency of *operations*, and (3) the *compliance* with applicable laws and regulations.

5.1 New European views on internal control systems

For a long time, the EU only focused on appropriate corporate disclosure rules and neglected the requirement for management systems to endorse the reliability of the reporting and internal control framework. However, the European Union has recently become more active in a number of areas such as company law, accounting, and auditing law.[67] The High Level Group of Company Law Experts, which was installed after the defeat in the European Parliament of the proposal for a take-over directive, recommended in its 2002 final report that companies disclose information on their risk management systems (or disclose the absence of such systems) in an annual corporate governance statement.[68] The board of directors should be collectively responsible for the system, and the audit committee must have a pivotal role in monitoring the company's internal audit procedures and its risk management system.[69] In its 2003 communication to modernise company law and enhance corporate governance in the EU, the European Commission endorsed the proposals of the High Level Group. The European Commission supported the disclosure requirements on the existence and nature of risk management systems and the duty of audit committees to monitor the system.[70] The European Commission emphasized the importance of including in the annual corporate governance statement information on how the company has organized itself to establish and maintain an *effective* internal control system, because of its essential role in restoring public confidence.[71] In addition, within Europe, industry specific requirements of internal control

[67] Notwithstanding these activities, large parts of the mentioned areas remain outside the scope of the European legislator and are firmly controlled by the national legislator for several reasons (for an analysis, see C. W. A. Timmermans, Company Law as Ius Commune?: First Walter van Gerven Lecture, 3 (Wouter Devroe & Dimitri Droshout eds., 2002), available at: http://www.law.kuleuven.ac.be/ccle/pdf/wvg1.pdf.)

[68] The High Level Group of Company Law Experts, *A Modern Regulatory Framework for Company Law in Europe*, Brussels, 4 November 2002, pp. 46-47. The High Level Group explicitly declared it considered additional study to be required to decide whether such a system should be mandatory.

[69] The High Level Group of Company Law Experts, *A Modern Regulatory Framework for Company Law in Europe*, Brussels, 4 November 2002, pp. 67 and 71.

[70] Communication from the Commission to the Council and the European Parliament, *Modernising Company Law and Enhancing Corporate Governance in the European Union - A Plan to Move Forward*, [COM(2003) 0284 final], 21 May 2003, pp. 12 and 15.

[71] See subsection 3.1.1, footnote at (b) of the Communication from the Commission to the Council and the European Parliament, *Modernising Company Law and Enhancing Corporate Governance in the European Union - A Plan to Move Forward*, [COM(2003) 0284 final], 21 May 2003.

and compliance were developed, in particular in the energy industry, where, as in the financial industry, compliance officers are considered indispensable to the proper functioning of energy providers.[72]

The revitalised efforts of the European Commission to harmonize large parts of company, securities, and accounting law encountered several hurdles and delays due to the opposition of EU member states. However, as in the US, scandals compelled the EU to react. In the first years of this century, the EU issued three directives and one recommendation in the field of securities and company law, as well as several different measures in specific industries, that address risk management and internal control systems within the corporate organisation. These directives, recommendation, and some industry-specific measures will be discussed in the next subsections.

5.2 The Transparency Directive

The 2004 Transparency Directive requires that a company's annual report include "a description of the principal risks and uncertainties that [it] face[s]".[73] The interim management report included in the half-yearly financial report must also provide information on the "principal risks and uncertainties for the remaining six months of the financial year".[74] The companies that must meet these requirements are issuers whose securities have been admitted to trading on a regulated market situated or operating within an EU member state.[75] The requirement to disclose the principal risks and uncertainties obliges companies to install at least a *risk and uncertainty detection system*.

Unfortunately, the directive provides no additional information as to what is considered a risk or uncertainty, nor when it should be considered *principal.* It is likely that this requirement

[72] See, for example, the proposal for a directive of the European Parliament and of the Council amending Directive 2003/54/EC concerning common rules for the internal market in electricity, [COM(2007) 528 Final 2007/0195 (COD)], 19 September 2007.

[73] Article 4, paragraph 2, subpart c, 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.

[74] Article 5, paragraph 4, Directive 2004/109/EG.

[75] Article 1, paragraph 1, Directive 2004/109/EG.

refers partly to the requirements in the Prospectus Directive 2003/71/EC and Commission Regulation 809/2004 that oblige companies to include risk factors in the prospectus.[76] 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.[77] Commission Regulation 809/2004 further differentiates between different types of issuers and securities regarding the disclosure of risk factors.[78]

Differences may exist between the requirements for the description of risks in the annual report and the risk factors in the prospectus. The annual report only has to report on the *principal* risks whereas the prospectus must refer to *specific* and *material* risks. It is safe to assume that risks that are not material can be precluded from the principal risks list, but neither does the principal risks list have to include all material risks. In addition, unlike *specific*, *principal* does not seem to preclude risks that are general to the market, industry, securities, etc. Also, the annual report has to provide information on risks and *uncertainties* whereas the prospectus, according to the Commission Regulation, limits the disclosure requirement to risks.[79]

As the EU is familiar with the concept of *materiality*,[80] the choice of the European Parliament and Council to require the disclosure of *principal* risks implies different meanings of the

[76] 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.)

[77] 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.

[78] The Share Registration Document must contain a risk factor section with a "prominent disclosure of risk factors that are specific to the issuer or its industry;" the Share Securities Note a section with the prominent disclosure of risk factors that are material to the securities being offered and/or admitted to trading in order to assess the market risk associated with these securities; the Debt and Derivative Securities Registration Document a section with prominent disclosure of risk factors that may affect the issuer's ability to fulfil its obligations under the securities to investors, etc.

[79] The Prospectus Directive requires the disclosure of *essential characteristics* and risks.

[80] To give but one example, the prospectus regulation requires the disclosure of "material" contracts that are not in the ordinary course of business in the Debt and Derivative Securities Registration Document (see Commission Regulation (EC) No 809/2004 of 29 April 2004).

words used. For the purpose of this paper, the assumption is that *principal* is related to the different categories as defined in the COSO frameworks, i.e. strategy, operations, reporting, and compliance. Principal risk must, however, not be reduced to the likelihood that there is a general default, to differentiate this risk from other types, such as currency risk, country risk, and inflation risk.

According to the Transparency Directive, uncertainties must be distinguished from risks. Where risk is defined as a measurable probability of an adverse event, uncertainty is broader and comprises the impossibility to describe and/or assess the (probability of an) outcome or event due to its non-quantitive nature.[81] However, IAS 1 can provide guidance to describe the uncertainties the Transparency Directive refers to in the annual and interim report. It requires that companies "disclose information about the assumptions it makes about the future, and other major sources of estimation uncertainty at the end of the reporting period, that have a significant risk of resulting in a material adjustment to the carrying amounts of assets and liabilities within the next financial year."[82] IAS 1 offers an approach to address the *uncertainty* to which the Transparency Directive refers. It relates to the anticipated effects of uncertain future events and requires most difficult, subjective, or complex assessments by the management.

The requirement to disclose the principal risks and uncertainties has no counterpart in SOX. A comparable rule can be found in Section 303 that deals with management's discussion and analysis of the financial condition and the results of operations of Regulation S-K. The management report must include information on the material events and uncertainties that are known to management and can cause the financial information to be less indicative of future results and condition.[83] The difference between the two requirements is clear. Section 303 specifically refers to *financial* information, whereas the Transparency Directive refers to principal risks in general. The US regulation limits the disclosure requirement to risks and uncertainties *that are known to management*, whereas the EU directive is not limited to these

[81] For a discussion of both notions, see F. Knight, *Risk, Uncertainty and Profit*, Hart, Schaffner & Marx: Boston, 1921.

[82] IASC, "IAS 1 Presentation of Financial Statements", *Technical Summary*, as at 1 January 2008, p. 2, see <http://www.iasb.org/IFRS+Summaries>.

[83] Title 17 (Commodity and Securities Exchanges), Part 229 (Regulation S-K), Item 303 (Management's discussion and analysis of financial condition and results of operations) of the Code of Federal Regulations, § 229.303. See "Instructions to paragraph 303(a)", under no. 3.

risks. Next, in the US only those events and uncertainties that make the financial information regarding future developments less indicative need to be disclosed. The EU obliges companies to disclose all principal risks whether or not they are likely to influence reported future developments. Lastly, the US regulatory framework requires management to assess the risks and uncertainties, whilst the EU approach leaves that assessment to the reader of the information.

5.3 The 2006 amendment to the Accounting Directives

The 2006 amendment to the Fourth and Seventh company law directives requires an annual corporate governance statement from companies whose securities are admitted to trading on a regulated market. 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."[84] 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.[85]

Internal control and risk management must provide reasonable assurance that the entity's objectives will be met. However, the directive limits the reporting to the application of the system to the financial reporting process. Hence, the directive requires reporting of the main features of the system so as to provide reasonable assurance of the effectiveness of the financial reporting process.

Superficially, the directive's requirement resembles the US SOX 302 and 404 requirements but the EU and US rules are far from identical and the former is less clear. The EU rule is limited to the description of the main features of the system for financial reporting. Theoretically, this directive does not require the establishment of such a system. However, it

[84] 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.

[85] Article 2, paragraph 2, Directive 2006/46/EC.

is highly unlikely that a company can comply with its financial reporting requirements and find an auditor to certify these accounts if the company operates without any kind of internal control and risk management system for the financial reporting process.

So, in the EU, the system that guarantees that reasonable assurance that objectives can be reached must be described in its main features. The following items can be considered minimum requirements to be disclosed in the annual corporate governance statement:

- The board of director's policy on risk management and internal control for financial reporting;
- The board's assessment of the key areas of internal control and risk management of the financial reporting system;
- The mechanisms in the systems regarding:
  - the identification and documentation of principal risks for the financial reporting system;
  - risk-addressing mechanisms (e.g., mitigation, insurance, acceptance);
  - monitoring;
  - reporting system regarding the financial reporting process;
  - the availability of sufficient human and material resources;
  - the education and training of employees and officers;
- The audit committee's oversight procedures;
- The external auditor's assessment.

The aforementioned minimum requirements combine two features of the system: its structure and its process. The board, the audit committee, management, and in particular the internal auditors and the external auditor are all part of the system. The process refers to the different steps to provide the reasonable assurance of reliable financial reports as identified in different frameworks, such as the COSO reports.

An inappropriate description of the main features of the internal control and risk management system for financial reporting will result in collective liability of the members of the administrative, management and supervisory bodies of the company. Unlike in the US, the failure to ensure the existence of an adequate system will not result in liability under this EU

directive as long as the main features of the system in relation to the financial reports are disclosed.[86]

5.4 The Audit Directive

Whilst the former two EU directives primarily discuss the disclosure of information on risks and risk management systems, respectively, 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.[87] 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."[88]

The latter requirement seems to resemble SOX Section 404 (b). In the US, the auditor must attest to and report on the management assessment of the effectiveness of the internal control structure and procedures for financial reporting. However, there are several differences between both regulations. In the US, the auditor has to deliver an attestation, whereas the European auditor must only report to the audit committee. Next, the European auditor must report the material weaknesses but has no monitoring duty regarding the effectiveness check by management. According to the EU Audit Directive, monitoring the effectiveness of the system in relation to financial reporting remains the sole duty of the audit committee. This difference is related to another distinction between the two systems. In the US, management must provide an assessment of the effectiveness. In the EU, the assessment of the effectiveness of the internal control system regarding financial reporting does not, at first sight, seem to be a requirement. The amendments to the Fourth and Seventh company law

[86] As long as other legal requirements are satisfied.

[87] 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.

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

directives require that the main features of the internal control system be reported. The purpose of the system is to provide reasonable assurance that corporate financial reporting processes are effective. It can be argued that an effectiveness assessment is required but that it should not necessarily be performed by management, nor on a yearly basis, as is the case in the US. The European Commission considers it the duty of the audit committee to address these issues at its discretion.[89]

This issue was taken up by the European Corporate Governance Forum, a body established by the European Commission in 2004 to examine best practices in EU member states with a view to enhancing the convergence of national corporate governance codes and providing advice to the Commission. In its *Statement on Risk Management and Internal Control*, the Forum confirmed that company boards are responsible for monitoring the effectiveness of internal control systems but that there is no need to introduce a legal obligation for boards to certify the effectiveness of internal controls at EU level.[90] The Forum came to that position after an assessment of the benefits and the costs of this additional requirement. The Forum therefore recommends that EU member states do not introduce a duty of certification.

The former requirement, i.e. to monitor the financial reporting process as well as the internal control system, significantly increases the responsibility of the audit committee. According to Article 41 of the 2006 Audit Directive the audit committee must not only monitor the effectiveness of the internal control system of financial reporting, but the effectiveness of all internal control systems. The recital is less clear where it distinguishes between the audit committee and effective internal control systems. The Commission considers both elements as essential conditions for a good internal governance system.

In the recitals of the 2006 amendment to the Fourth and Seventh company law directives, the collective responsibility of the board is stressed. Article 41, paragraph 2 of the Audit Directive also emphasises the responsibility of the board members. In addition, the Audit Directive requires the audit committee to take care of the monitoring of the effectiveness of the internal control systems. It is reasonable to assume that the member states will establish an

[89] Cf. infra.

[90] Paragraph 6, European Corporate Governance Forum, *Statement on Risk Management and Internal Control*, Brussels, June 2006. The full text of the statement is available at: <http://ec.europa.eu/internal_market/company/ecgforum/index_en.htm>.

appropriate relationship between responsibility and liability of board members, in particular malpractice liability with regard to monitoring the effectiveness of the internal control.

5.5 The Commission Recommendation

In February 2005, the European Commission issued a recommendation on independent directors and committees of the board.[91] The recommendation is broader than the scope of the 2006 Audit Directive, which focuses on monitoring the effectiveness of the internal control and the risk management systems as the main duties of the audit committee. The recommendation contains several principles to structure the role of the audit committee. This committee should assist the board in its task to, e.g.:[92]

- 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.

Both the Audit Directive 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 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

[91] 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.

[92] Commission Recommendation, OJ L 52 of 25 February 2005, Annex I, Committees of the (supervisory) board, p. 61.

system but the committee only has to assess the effectiveness of the internal audit function and external audit process.[93]

5.6 Industry-related approaches

The scope of the aforementioned directives is general. In short, almost all listed companies and public interest entities must comply with their requirements. However, the EU has also developed industry-specific rules. For instance, in the financial industry, the Mifid Directive is well known; in the chemical industry, companies are preparing for the implementation of the REACH Regulation; in the utilities industries, special compliance programs are being studied. A large group of companies have to comply not only with the general internal control, risk management, and compliance programs but also with these industry-specific rules.

In the financial industry, investment firms "shall have sound administrative and accounting procedures, internal control mechanisms, effective procedures for risk assessment, and effective control and safeguard arrangements for information processing systems".[94] Investment firms provide investment services on a regular basis.[95] Investment services include the reception, transmission, and execution of orders, and investment advice.[96] Credit institutions that provide investment services are also required to use sound procedures. Generally, credit institutions need "robust governance arrangements, which include a clear organisational 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, and adequate internal control mechanisms, including sound administrative and accounting

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

[94] Directive 2004/39/EC of the European Parliament and of the Council of 21 April 2004 on markets in financial instruments amending Council Directives 85/611/EEC and 93/6/EEC and Directive 2000/12/EC of the European Parliament and of the Council and repealing Council Directive 93/22/EEC, OJ L 145 of 30 April 2004, p. 1.

[95] Article 4, paragraph 1 of Directive 2004/39/EC.

[96] See Annex I, section A of Directive 2004/39/EC.

procedures."[97] These arrangements must be "comprehensive and proportionate to the nature, scale and complexity of the credit institution's activities."

The Mifid Directive and the Banking Directive require companies in the financial industry to establish overall internal control and risk management systems, including all operational activities.[98] However, unlike in the aforementioned general directives, the Mifid Directive does not require an effectiveness assessment by management or an audit committee. Nonetheless, this monitoring provision can be found in Directive 2006/73/EC where specific and detailed risk management and internal audit procedures are prescribed.[99] Senior management, the persons who direct the business, are responsible for compliance. Also, the supervisory authority has specific powers and rights to assess the conduct of the business.[100] Next to the general internal control and risk management requirements in the financial services industry, the Mifid Directive also compels investment firms to take into account specific requirements, such as the best-execution rule, procedures to demonstrate compliance,[101] and the non-discriminatory policy for the execution of orders by systemic internalisers.[102]

---

[97] Article 22 of Directive 2006/48/EC of the European Parliament and of the Council of 14 June 2006 relating to the taking up and pursuit of the business of credit institutions, OJ L 177 of 30 June 2006, p. 1.

[98] Equivalent requirements are given in other directives related to the financial industry. See, for example, Article 9 of Directive 2002/87/EC of the European Parliament and of the Council of 16 December 2002 on the supplementary supervision of credit institutions, insurance undertakings and investment firms in a financial conglomerate and amending Council Directives 73/239/EEC, 79/267/EEC, 92/49/EEC, 92/96/EEC, 93/6/EEC and 93/22/EEC, and Directives 98/78/EC and 2000/12/EC of the European Parliament and of the Council. Financial conglomerates must have an internal control mechanism to identify and measure all material risks incurred and to appropriately relate their own funds to risks as well as sound reporting and accounting procedures to identify, measure, monitor, and control intra-group transactions and risk concentration.

[99] Articles 7 and 8 of Commission Directive 2006/73/EC of 10 August 2006 implementing Directive 2004/39/EC of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive, OJ L 241 of 2 September 2006, p 26.

[100] See Article 63, paragraph 3 (a) of Directive 2004/39/EC.

[101] See Article 21 of Directive 2004/39/EC.

[102] See Article 25, paragraph 2 of Commission Regulation (EC) No. 1287/2006 of 10 August 2006 implementing Directive 2004/39/EC of the European Parliament and of the Council as regards recordkeeping obligations for investment firms, transaction reporting, market transparency, admission of financial instruments to trading, and defined terms for the purposes of that Directive, OJ L 241 of 2 September 2006, p. 1.

Another industry-specific set of rules is the 2006 REACH Regulation No. 1907/2006.[103] It requires the chemical industry to assess and manage the risks related to substances and preparations it manufactures and places on the market. Its aim is to improve the protection of human health and of the environment. Substances and preparations must be registered before being manufactured or placed on the market. They must be identified, described, and classified, and if additional conditions are met, a chemical safety report must be issued and appropriate measures to adequately control the risks identified in the chemical safety assessment must be applied.[104] Many other provisions require additional assessments and evaluations.[105] This legislation compels many industrial companies to develop additional operational control mechanisms in their production chain to meet all the requirements. Other industries are also familiar with similar requirements. Under Regulation No. 178/2002, businesses in the food industry are required to ensure that foods and feeds satisfy food law requirements, including the traceability of substances, and are required to have all information about food procession readily available through suitable systems.[106]

[103] Regulation (EC) No. 1907/2006 of the European Parliament and of the Council of 18 December 2006 concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH), establishing a European Chemicals Agency, amending Directive 1999/45/EC and repealing Council Regulation (EEC) No. 793/93 and Commission Regulation (EC) No. 1488/94 as well as Council Directive 76/769/EEC and Commission Directives 91/155/EEC, 93/67/EEC, 93/105/EC and 2000/21/EC.

[104] See Annex I for the general provisions on assessing substances and preparing the chemical safety reports of Regulation No. 1907/2006.

[105] See, for example, Article 22, under (e), Article 31, paragraph 9, under (a), Article 32, paragraph 1, under (d) and paragraph 3, under (a), Article 37, paragraph 5 and 6, Article 41, paragraph 1, under (c), Article 64, paragraph 4, under (a), Article 70 of Regulation No. 1907/2006.

[106] Regulation (EC) No. 178/2002 of the European Parliament and of the Council of 28 January 2002 laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety, PB L 31, 1 February 2002, p. 1.

6. Assessing the EU and US approaches to internal control and risk management

Over the last years, the quantity of regulation related to internal control and risk management has been piling up. US companies have had to develop systems that at least meet requirements to identify risks, to report the main features of the control system for financial reporting, and to assess the effectiveness of this system. The EU legislator has also developed a new regulatory environment with risk management systems and internal control procedures (if starting from and with different motives). Some new requirements have introduced higher standards regarding the administration of companies. Others aim to reduce the probability of fraudulent activities and to restore trust in the financial markets. Yet other rules sensitize corporate constituents and third parties by requiring more reporting and disclosure. A last class of new rules seeks to enhance safety, competition, or other, more general purposes. No doubt, all these aims and ambitions are useful. However, the different rules lack consistency and require an individual hands-on implementation approach preventing a process-oriented implementation procedure.

Lately, in addition to and in light of the aforementioned internal control and risk management issues and rules, the focus has been on compliance risks. Compliance with legal rules is regarded as the primary area where risks have increased.[107] European regulatory authorities must ensure that companies engage in developing a coherent legal framework. The US regulatory framework can be useful for redirecting the EU approach to develop a more consistent framework. Such a framework must allocate duties and responsibilities to the different corporate constituents.

Figure 1 is a two-dimensional model of an internal control and risk management framework. The first dimension refers to the different steps to be taken in establishing an internal control and risk management framework. The system must first be initiated and the different systems

[107] Ernst & Young, *Board members on risk – leveraging frameworks for the future*, 2006, p. 5. This shift can, for example, be seen in the Fortune 200 companies almost all of which have issued a business code. The most frequently cited argument for the development of such a code is compliance with legal requirements. See KPMG, *Business Codes of the Global 200: Their Prevalence, Content and Embedding*, 2008, p. 8.

must be identified, based on the classification along three of the four COSO-defined goals.[108] The identified systems must then be assessed as well as monitored, and, finally, the framework must include the reporting on the systems and their effectiveness. The second dimension refers to the different parties involved from the corporate law perspective. Senior management can be further divided into CEO, internal auditor, compliance officer, etc. The initiation and identification of risks and the relevant management system can be expected to be the responsibility of senior management in cooperation with the board of directors. With the assistance of senior management (e.g., the chief risk officer), the board of directors identifies the risks and initiates the internal control and risk management systems with the ultimate aim of meeting the strategic, operational, and financial reporting goals. The operationalisation and assessment of the systems as well as the responsibility of addressing the risks should be the duty of senior management in collaboration with the board of directors. The audit committee is responsible for the supervision and monitoring of the initiated financial reporting system and the well-functioning of this system, including the assessment of the results and the way the organisation mitigates the weaknesses of the financial reporting system. The audit committee should also address the effectiveness of the system. Other committees of the board or the board itself should be responsible for a similar monitoring process for the strategic and operational management systems. Final responsibility for reporting the different steps of the internal control remains with the board of directors, which should ensure compliance with the regulatory reporting framework. Finally, the external auditor monitors the adequacy of the control system for financial reporting.

[108] For the sake of simplicity, the fourth goal, compliance, is not included in this model. Compliance with laws and regulations must be taken into consideration when the financial, strategic, and operational systems are identified and initiated, but the compliance system should also cover integrity risks at the four levels of the model throughout the organisation.

Figure 1: Regulatory internal control and risk management framework

			Senior management	Board	Audit committee	Auditor
Level 1: initiate/identify						
	Risks/uncertainties					
	Strategic ICS*/RMS*					
	Fin rep ICS/RMS					
	Operational ICS/RMS					
Level 2: assess/operate						
	Risks/uncertainties					
	Strategic ICS/RMS					
	Fin rep ICS/RMS					
	Operational ICS/RMS					
Level 3: monitor						
	Risks/uncertainties					
	Strategic ICS/RMS	general				
		effectiveness				
	Fin rep ICS/RMS	general				
		effectiveness				
	Operational ICS/RMS	general				
		effectiveness				
Level 4: report on						
	Risks/uncertainties					
	Strategic ICS/RMS	general				
		effectiveness				
	Fin rep ICS/RMS	general				
		effectiveness				
	Operational ICS/RMS	general				
		effectiveness				

* ICS: internal control system

* RMS: risk management system

The US regulatory framework addresses parts of the duties as presented in Figure 1. First, the FCPA requires a system of internal accounting controls. Notwithstanding the emphasis of US rulemaking on the reporting of financial information, the sentencing guidelines underline the importance of an effective program to prevent and detect violations of the law. In its *Caremark* decision, the court states that boards must assure themselves that "information and reporting systems exist in the organization that are reasonably designed to provide to senior

management and to the board itself timely, accurate information sufficient to allow management and the board, each within its scope, to reach informed judgements concerning both the corporation's *compliance with law and its business performance.*"[109] The court identifies the duty to put internal controls in place in order to reach the goals of compliance with the laws and business performance. The US rulebook covers the level 1 and 2 themes of initiating and assessing appropriate internal control systems for financial reporting. The internal control system must be designed so as to reasonably discover internal control deficiencies, allowing management and the board to respond to red flags. If the systems are in place and reveal deficiencies that the board appropriately addresses, courts will not hold directors liable. Courts are also very reluctant to hold directors liable if the system, organised in a different way, would have revealed more deficiencies or if the systems in place comply with industry standards and practices, but do not reveal deficiencies. If systems do not prevent abuses and the directors cannot be unaware of the deficiencies of the system, the board will be liable. Similarly, if the system does not reasonably address deficiencies or is totally flawed, directors will be liable. In those circumstances, illegal conduct might occur and the directors would breach their duty of care. This approach results in a marginal assessment of the reliability of the system, the monitoring function. Before the enactment of SOX, this level 3 topic – monitoring the internal control over financial reporting – was only addressed in general terms by Regulation S-X. Assessing the effectiveness of the system prescribed by the sentencing guidelines to prevent and detect violations of law requires, in practice, an additional layer of monitoring that is itself not required. As with level 3, until SOX, level 4 – reporting on risks and systems – was only addressed in general terms. The MD&A requires reporting on events and uncertainties that materially affect the operating results or financial condition of the corporation. Reporting on the effectiveness of the system was, prior to SOX, not required.

SOX modified the US framework significantly by emphasising the level 1 and 2 issues and adding level 3 and 4 requirements to the internal control environment. At level 3, management, the board, audit committee, and auditors must address the (effectiveness of the) financial reporting system and the financial disclosure systems, and at level 4, management and auditors are involved in reporting on the effectiveness of the financial reporting system. Figure 2 summarizes these findings. The US approach resembles the general figure (Figure 1)

[109] Caremark International Inc. Derivative Litig., 698 A.2d 959, 970 (Del. Ch. 1996).

in part but deviates at two levels. First, the US emphasizes the responsibility of management reporting on the effectiveness of the financial reporting system. Second, the board is not involved in reporting on the internal control over financial reporting system. In addition, figure 2 shows that although the important role of management, as distinct from the role of the board of directors, seems neglected in corporate law in general, the FCPA and SOX (as well as the MD&A) requirements dealing with internal control and risk management emphasize the responsibility of senior management.

Figure 2: US framework on internal control and risk management

			Senior management (CEO/CFO)	Board	Audit committee	Auditor
Level 1: initiate/identify						
	Risks/uncertainties		ex. 303 MD&A*	8.01 (C) MBCA		
	Strategic ICS*/RMS*					
	Fin rep ICS/RMS		FCPA / 302 SOX 404 SOX			
	Operational ICS/RMS					
Level 2: assess/operate						
	Risks/uncertainties		ex. 303 MD&A			
	Strategic ICS/RMS					
	Fin rep ICS/RMS		FCPA / 302 SOX 404 SOX			
	Operational ICS/RMS					
Level 3: monitor						
	Risks/uncertainties		ex. 303 MD&A	8.01 (C) MBCA		
	Strategic ICS/RMS	general				
		effectiveness				
	Fin rep ICS/RMS	general	302 SOX		205 SOX[110]	Reg. S-X

[110] Additional requirements can be found in the stock exchange rulebooks.

		effectiveness	302 SOX 404 SOX	8.01 (C) MBCA		404 SOX
	Operational ICS/RMS	general				
		effectiveness		8.01 (C) MBCA		
Level 4: report on						
	Risks/uncertainties		303 MD&A / 409 SOX			
	Strategic ICS/RMS	general				
		effectiveness				
	Fin rep ICS/RMS	general	302 SOX			
		effectiveness	302 SOX 404 SOX			404 SOX
	Operational ICS/RMS	general				
		effectiveness				

* ICS: internal control system

* RMS: risk management system

* ex.: extracted

The EU regulatory framework significantly differs from the US approach. Figure 3 is an overview of the general requirements at EU level regarding internal control and risk management. The EU directives only cover a limited part of the internal control levels. The initiation and, in particular, the operational parts of the internal control framework are not explicitly addressed. From the Transparency Directive, requiring the disclosure of risks and uncertainties, it can be deduced that risks and uncertainties must be identified. As the party who is responsible for the identification procedure is not defined, it can be argued that it is the board of directors that is responsible for the identification of the risks and uncertainties and that their responsibility can be delegated. The Audit Directive attributes the duty to monitor the internal control system to the audit committee, composed of directors. Whereas the responsibility is identified, liability is not. The deficiency of the EU system – or rather the incompleteness – has been countered by the regulators in the member states.[111]

[111] Cf. infra.

Figure 3: EU framework on internal control and risk management

		Responsible persons	Senior management	Board	Audit committee	Auditor
Level 1: initiate/identify						
	Risks/uncertainties	ex. transp. dir.				
	Strategic ICS*/RMS*	ex. transp. dir.				
	Fin rep ICS/RMS	ex. transp. dir.		ex. 4-7 dir.		
	Operational ICS/RMS	ex. transp. dir.				
Level 2: assess/operate						
Level 3: monitor						
	Fin. report process				8 dir.	
	(Effectiveness) ICS				8 dir./recom.	
	Effectiveness IA* S/F				8 dir./recom.	
	(Effectiveness) RMS				8 dir./recom.	
	Effectiveness EA*				8 dir./recom.	
Level 4: report on						
	Risks and uncertainties	transp. dir.				
	Weakness IC for fin. rep.					8 dir.
	Features ICS for fin. rep.			4-7 dir.		
	Features RMS for fin. rep.			4-7 dir.		

* ICS: internal control system

* RMS: risk management system

* ex.: extracted

* IA: internal audit

* EA: external audit

In addition to these European rules, many EU member states have developed additional risk management and internal control requirements.[112] For example, in the Netherlands, the 2008 Dutch Corporate Governance Code (hereinafter: DCGC 2008) requires companies to have an internal risk management and control system that is suitable for the company.[113] The required

[112] For a detailed analysis of the variety in internal control and risk management provisions within multiple member states, see M. M. A. van Daelen, *Evolving Risk Management and Internal Control Provisions in EU member states*, forthcoming.

[113] Monitoring Commissie Corporate Governance Code, *The Dutch Corporate Governance Code - Principles of Good Corporate Governance and Best Practice Provisions* (DCGC 2008), December 2008. In June 2008, the Monitoring Committee proposed amendments to the former DCGC of 2003 (see Corporate Governance Code

system must at least make use of the following instruments: risk analyses of the company's operational and financial objectives, a code of conduct (published on the company's website), guides for the layout of the financial reports and the procedures to be followed in drawing up the reports, and a monitoring and reporting system.[114] The former DCGC[115] already introduced an "in control statement", which required the management board to declare in the annual report that the systems are adequate and effective.[116] The current DCGC reformed 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 worked properly.[117]

In the UK, the Combined Code requires the board to maintain a sound system of internal control and to annually review – and report to shareholders that they have done so – the effectiveness of the group's internal control system – covering all material controls, including financial, operational, and compliance controls – and risk management systems.[118]

The 2009 Belgian Code on Corporate Governance and its predecessor the Lippens Code[119] state that the board and the audit committee must make sure that risks can be assessed and managed. Statements on internal control and risk management have to be included in the annual report. The existence and functioning of an internal control system with adequate risk identification and risk management, including risks relating to compliance with existing legislation and regulations, must be reviewed.[120] Executive management must put internal

---

Monitoring Committee, *Report on the Evaluation and Updating of the Dutch Corporate Governance Code*, 4 June 2008).

[114] Best practice provision II.1.3 of the DCGC 2008.

[115] Commissie Corporate Governance, *The Dutch Corporate Governance Code - Principles of Good Corporate Governance and Best Practice Provisions* (DCGC 2003), 9 December 2003. This code came into effect from the financial year starting on 1 January 2004.

[116] Best practice provision II.1.4 of the DCGC 2003.

[117] Best practice provision II.1.5 of the DCGC 2008.

[118] Financial Reporting Council (FRC), *The Combined Code on Corporate Governance*, June 2008. See principle C.2 and provision C.2.1.

[119] Belgian Corporate Govemance Committee, *The 2009 Belgian Code on Corporate Governance*, March 2009 and Belgian Corporate Governance Committee, *The Belgian Code on Corporate Governance* (Lippens code), 9 December 2004.

[120] Principle 1, paragraphs 1.1, 1.3, and Appendix C, provision 5.2./14-5.2./16 of the 2009 Code.

controls – systems to identify, assess, manage, and monitor financial risks and other risks – in place without prejudice to the abovementioned monitoring responsibilities of the board and the audit committee.[121]

In France, the Financial Security Act of 1 August 2003[122] requires the chair of the board of directors to present a report on the internal auditing procedures of the company. The law of 3 July 2008[123] further developed the legal requirements as the chairman also needs to report on the internal control procedures and the risk management system that is in place. As the Financial Security Act does not specify which internal auditing procedures to refer to, most companies interpret the requirement in the broadest sense, reporting not only on the procedures to enhance the reliability of the financial reporting process, but also on other internal control procedures.[124] The effects of the law of July 2008 are not yet visible.

7. Concluding remarks

Both the US and the EU responded to the major failures around the turn of the century with additional regulations on internal control and risk management systems. These systems offer a framework that reflects a sound business practice, which was needed in order to restore public confidence. However, the US and EU approaches were, and still are, significantly different. The US focus is mainly on internal control systems for financial reporting, with legislation covering all the levels – initiate, assess, monitor, and report – of the model presented in Figure 1. The US requirements also show a distinction between monitoring and reporting on the system in general, on the one hand, and on the effectiveness of the system, on the other hand. The EU approach deals with a broader concept of internal control and risk management. The requirements focus on internal control and risk management covering financial reporting as well as the strategic, operational, and compliance systems. At EU level, monitoring of the effectiveness of the internal control, internal audit, external audit, and risk management systems is required. What is also required is the disclosure of information on (1) the

[121] Principle 6, paragraph 6.5 of the 2009 Code.

[122] Article 122 of Act 2003-706 of 1 August 2003, *French Official Gazette*, 2 August 2003.

[123] Article 225-37 Commercial Code as amended by Law 2008-649 of 3 July 2008 ("Loi DDAC"), *French Official Gazette*, 4 July 2008.

[124] For an analysis of the reports, see http://www-amf-france.org/documents/general/8587_1.pdf.

companies' overall risks and uncertainties, (2) the weakness in internal control relating to the financial reporting process, and (3) the main features of the companies' internal control and risk management systems relating to the financial reporting process.

Both approaches are incomplete – but not necessarily insufficient – in different areas. The US requirements provide a sound basis for an internal control system for financial reporting system at all levels, from initiating to reporting. The sentencing guidelines deal with fraud, and indirectly with financial reporting, by requiring organisations to have an effective program to prevent and detect violations of law. In essence, the US framework helps companies to provide investors with reliable information on their current and future financial condition. The focus on this kind of information provides a clear direction. However, to disclose reliable information on their financial condition, companies may also need to have strategic and operational internal control systems in place, since those systems are considered essential for making a complete financial assessment. For example, the board's oversight responsibility as stipulated by the MBCA includes giving attention to the overall business performance and plans as well as to the major risks to which the corporation is or may be exposed. To sum up, the US approach to internal control consists of regulating the financial reporting process and leaving the strategic and operational internal control and risk management processes untouched. It is left to the companies to implement these processes in order to properly fulfil their responsibilities for their financial reporting system and, more generally, in order for their boards to exercise their oversight responsibilities.

The requirements at EU level are more principle-based and do not explicitly refer to the initiation and operational part of the internal control framework, nor do they fully deal with all issues at the reporting level. The EU requirements offer more flexibility to develop an appropriate internal control environment. However, this approach lacks consistency for the EU member states. Besides the monitoring of the financial reporting process, the monitoring of the effectiveness of the company's overall internal control, internal audit, and risk management systems is required. The reporting level only focuses on risk and uncertainties in general, the weaknesses in internal control, and the main features of the system for financial reporting. The principle-based approach has played a guiding role for the EU member states. In order to ensure that companies fulfil their monitoring obligations, most member states have added requirements in laws, regulations, and codes to deal with levels 1 and 2 (i.e., initiate/identify and assess/operate internal control systems). Generally, the framework is

further completed by member states requiring companies to have, maintain, monitor, and/or report on internal systems for financial, operational, strategic, and compliance controls. It is not yet clear whether the divergent requirements in different member states will slow down the creation of a level playing field in the EU for companies. The total EU framework, including the requirements of the EU and the EU member states, has a much broader – and more burdensome – scope than the US framework.

Besides the diverging levels covered by regulations, the duty to initiate, assess, monitor, and report is imposed on different parties. In the US framework, senior management is responsible for initiating, assessing, monitoring, and reporting on the internal control system for financial reporting. The duties cover the system in general as well as its effectiveness. The auditor also plays a role in monitoring and reporting on the internal control system for financial reporting. Furthermore, the audit committee must monitor both the accounting and financial reporting processes of the issuer and the audit of the financial statements of the issuer. Strikingly, the board's duty is mostly limited to the monitoring level and it is not involved in reporting on internal control.

The EU framework imposes obligations on different parties. The audit committee is solely responsible for all monitoring duties. The duty covers the financial reporting process, (effectiveness of) the internal control system, effectiveness of the internal audit system and function, (effectiveness of) the risk management system, and effectiveness of the external audit. The external auditor has to report on weaknesses in the internal control relating to the financial reporting process. The only explicitly described duty of the board is to report on the main features of the internal control and risk management systems relating to the financial reporting process. The persons responsible for reporting on risks and uncertainties in general can be all or some of the board members, senior management, or other persons within the company, depending on the choices made by member states in implementing the Transparency Directive. To conclude, where the US framework mostly imposes duties on senior management, in the EU, the framework mainly concentrates on the duties of the audit committee.

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

www.ecgi.org\wp

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