COMPARISON OF RISK MANAGEMENT REGULATION FROM A CORPORATE GOVERNANCE PERSPECTIVE WITHIN THE GERMAN AND UNITED STATES LEGAL AREAS

Remmer Sassen *

Abstract

Risk management is one of the main corporate governance components or management tasks. This paper details a comparison of risk management regulation from a corporate governance perspective of listed stock corporations in Germany and the United States (U.S.). Obviously, there are differences and commonalities between the national legal norms and the regulatory levels of risk management in both countries. The comparison helps to understand different traditions and practices in terms of how significant corporate governance rules are for risk management. Therefore, this article intends to inspire future research on the regulation of risk management across different regions and explore the relevance of national interests in the regulation of risk management. A principal finding of the comparison is that the U.S. corporate governance system seems to be more strongly regulated than the German system. This results from the powerful and coordinating role of the U.S. Securities and Exchange Commission (SEC). Thus, the seemingly more liberal system of non-binding standards in the U.S. has a higher impact on the regulation of risk management than in Germany.

Key Words: Risk Management, Regulation, Corporate Governance, Germany, US, Legal Area

** Chair of Auditing, Institute of Auditing and Taxation, University of Hamburg*
Tel.: +49 (0) 40-42838 7966
Fax: +49 (0) 40-42838 6714
E-mail: Remmer.Sassen@wiso.uni-hamburg.de

1 Introduction

Risk management is an important component of corporate governance (Daelen and Ven 2010, p. 2). According to Shleifer and Vishny (1997), corporate governance deals with the way in which investors ensure themselves a return on their investment (p. 737) (Bebchuk and Weisbach 2010, p. 940). The Cadbury Commission (1992) interprets corporate governance as the system by which companies are directed and controlled (para. 2.5). Thus, rules and guidelines affecting corporate governance lead to a more effective management and monitoring of companies (Hopt 2011, pp. 448–449). Consequently, an appropriate corporate governance structure is important for risk management (Tao and Hutchinson 2013, p. 83). Obviously, there are interrelations and interdependencies between corporate governance and risk management (Quon, Zéghal, and Maingot 2012, p. 95). Many scholars have pointed out that failures of corporate governance and risk management are key causes of the recent financial and economic crisis (e.g., Pirson and Turnbull 2011, p. 459; Quon, Zéghal, and Maingot 2012, p. 95; Xu, Grove, and Schaberl 2013, p. 104). Because of this and recent corporate scandals worldwide, many legal and quasi-legal norms and reforms of various developed nations determine the necessity of appropriate risk management and internal control systems (Sarens and Christopher 2010, p. 289). The subjectivity of this area and different interests of national regulators lead to different national levels of regulation. Some regulators use mandatory rules, whereas others tend to use more voluntary corporate governance guidelines in order to ensure that companies implement and execute an appropriate form of risk management.

The following discussion focuses on the relevance of regulations for risk management through corporate governance rules and guidelines in Germany and the U.S. considering the direct and implicit effects of recent corporate governance reforms. There are organizational differences in the German and U.S. legal systems regarding stock corporations. In Germany, there is a two-tier system for stock corporations. It includes a separation between the management board and supervisory board. The U.S. stock corporation is organized as a one-tier system. The role of management and supervision is contained in one board of directors. This fundamental organizational distinction and differing legal or quasi-legal rules have various

effects on the integration of risk management into the German and the U.S. corporate governance system. This paper does not focus on the respective rules for financial institutions as there are comprehensive special requirements for risk management owing to the economic importance and systemic risks of this sector.

The purpose of this paper is to illustrate the risk management regulation from a corporate governance perspective including the recent regulatory reforms and guidelines within the German legal system and to compare these rules to the U.S. legal system. It will examine the direct and implicit regulations of risk management as one of the main management tasks to increase shareholder value; the institutional structure of a listed stock corporation; the link between financial reporting, publicity, and risk management; and the relevance of the external corporate monitoring system in risk management. This will be done for both legal systems in order to show the relevance of legal norms in risk management. It includes an examination of the integration of risk management into the corporate governance system of German and U.S. stock corporations. Finally, this paper compares both systems in terms of the relevance of legal norms and guidelines for risk management in order to analyze the existing differences and commonalities. With this approach, the level of regulation of risk management in both countries can be shown on a qualitative basis.

This paper contributes to the literature on risk management by presenting a comparison of risk management regulation from a corporate governance perspective. This is useful in understanding other approaches and identifying new developments. This is a new approach to compare the level of regulation of risk management between Germany and the U.S. by showing the relevance of corporate-governance-oriented rules and guidelines in risk management. Moreover, it inspires future research in this area.

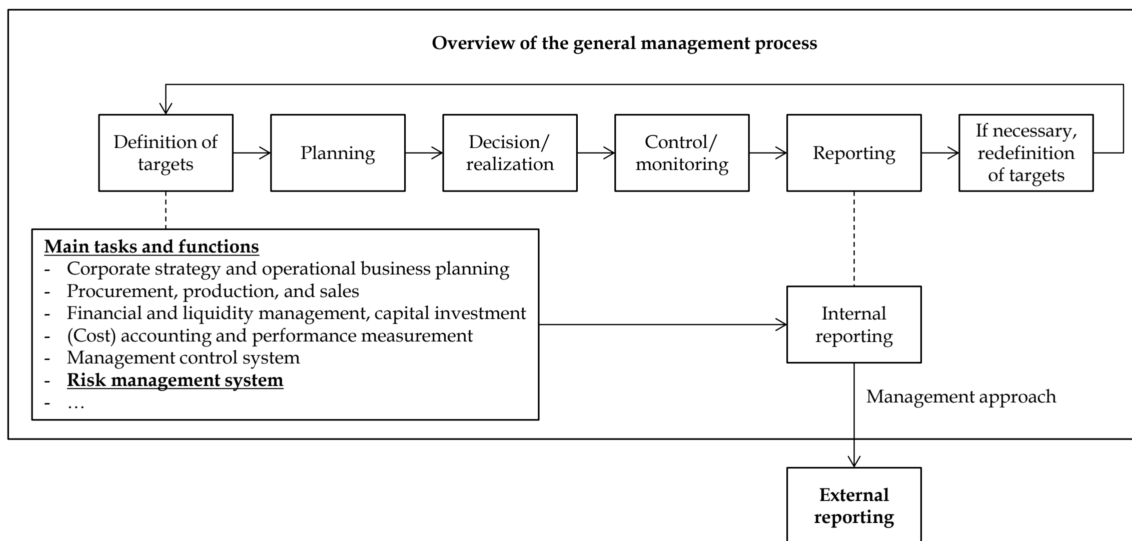
The remainder of this paper is organized as follows. Section 2 contains a theoretical foundation of enterprise risk management as a component of corporate governance. Sections 3 and 4 analyze risk management as a component of the corporate governance system of a German and U.S. stock corporation. Finally, a comparison of both systems as well as further conclusions, limitations, and future research needs are postulated in Section 5.

2 Theoretical foundation of enterprise risk management as a corporate governance component

The primary task of a business corporation and its management is to increase the value of its shareholders' investment (Rappaport 1986, p. 1). Consequently, the primary goal of enterprise risk management is to maximize shareholder values (e.g., Brezeanu, Al Essawi, Poanta, and Badea 2011, p. 50; Quon, Zéghal, and Maingot 2012, p. 95). In a public corporation, the decision management and the decision control as well as investment and risk-bearing by public shareholders are usually separated (Fama and Jensen 1983, p. 301). Acharya, Myers, and Rajan (2011) offer clear evidence that most shareholders have little control over boards and that many boards are generous toward corporate leadership (p. 689). Therefore, it is possible that managers are not faithful servants of the shareholders because of their own interests (Shleifer and Vishny 1997, p. 743). Usually management compensation is used to mitigate agency problems in order to align management interests with those of the shareholder. (Shleifer and Vishny 1997, p. 744). Alternatively, lawmakers have the option to enact a law to mitigate these problems. One opportunity for said mitigation is to establish corporate governance rules on risk management in order to protect the shareholders.

To increase shareholder value, the management establishes a management process (Figure 1) that can be performed as follows: definition of targets, planning, decision and realization, control and monitoring, reporting and, if necessary, redefinition of targets (Wöhe and Döring 2013, pp. 47–49). Subtasks of management usually affect corporate strategy and operational business planning, procurement, production and sales, financial and liquidity management, capital investment, (cost) accounting and performance measurement, risk management, and so on. These subtasks generally have analogous processes. Furthermore, there are interactions between these subtasks and management functions (Günther 2013, p. 282). According to Quon, Zéghal, and Maingot (2012), effective risk management is a process that requires a firm's management to identify and assess the collective risks that affect firm value and apply an enterprise-wide strategy to manage those risks (p. 95). Other company-specific tasks, such as the development of internal reporting structures and their implementation, are part of the management process. Moreover, the external reporting is usually based on internal reporting (management approach) (Velte 2008, pp. 133–134).

Figure 1. Overview of the general management process



Management decisions serve corporate purposes only, with a focus on maximizing shareholder value. Legal rules are only of secondary interest in this context. Risk management, on the other hand, is both a primary task of management and is regulated by legal rules and guidelines. Thus, risk management is a central and important management and corporate governance task as it sustains value creation (Froot, Scharfstein, and Stein, p. 1629; Pirson and Turnbull 2011, p. 459). Its main aim is to stabilize the firm and to ensure sustainable earnings. Recently, there have been different legal influences on risk management in Germany as well as the United States. This means that there are external legal factors that have an impact on the internal (risk) management process of the company as secondary conditions. (Freidank and Sassen 2012, p. 167). Firstly, there are legal requirements to establish a risk management. Secondly, financial reports have to contain more and more risk-relevant information (Ryan 2012, p. 296). This paper will not focus in detail on risk-relevant accounting standards (for use of fair values, see, e.g., Ryan 2012, pp. 304–307). They are only mentioned in passing or by way of example. Thirdly, auditors and other regulatory authorities have to review this information. Because of these different legal requirements that affect risk management, the next section analyses risk management as a component of the corporate governance system of a German stock corporation including the aforementioned legal requirements. The same procedure is carried out for the U.S. system in section 4.

3 Risk management as a component of the corporate governance system of a German stock corporation

This section analyzes how risk management can be integrated into the corporate governance system of a listed stock corporation in order to show the direct and implicit links, relationships, interactions, and dependencies between risk management and the corporate governance components. The analysis is based on corporate-governance-oriented norms (legal rules and quasi-legal standards) in relation to their relevance to risk management. Important rules and standards are the German Stock Corporation Act [Aktiengesetz (AktG)] and complementary guidelines of the German Corporate Governance Code [Deutscher Corporate Governance Kodex (DCGK)] as well as the German Commercial Code [Handelsgesetzbuch (HGB)]. The DCGK contains different recommendations to clarify the obligations of the management and supervisory board "[…] to ensure the continued existence of the enterprise and its sustainable creation of value in conformity with the principles of the social market economy (interest of the enterprise)." (DCGK 2013, Foreword). Some sections of the DCGK address risk management explicitly. The "comply or explain" principle (Sec. 161(1) AktG) allows companies to deviate from the DCGK when it is justified by the circumstances and when the company explains the deviation. The declaration of conformity has to be published as part of the management report (Sec. 289a(2) HGB). Consequently, companies have an implicit obligation to use the DCGK recommendations. Furthermore, there are accounting and reporting standards issued by the Accounting Standards Committee of Germany (Deutsches Rechnungslegungs Standards Committee) and auditing standards issued by the Institute of Public Auditors in Germany (Institut der Wirtschaftsprüfer). These complementary standards and the relevant norms for financial institutions such as the German Banking Act (Kreditwesengesetz) or the Minimum Requirements for Risk Management (Mindestanforderungen an das Risikomanagement) are not analyzed here in detail.

Firstly, this section focuses on provisions of the AktG and complementary guidelines of DCGK

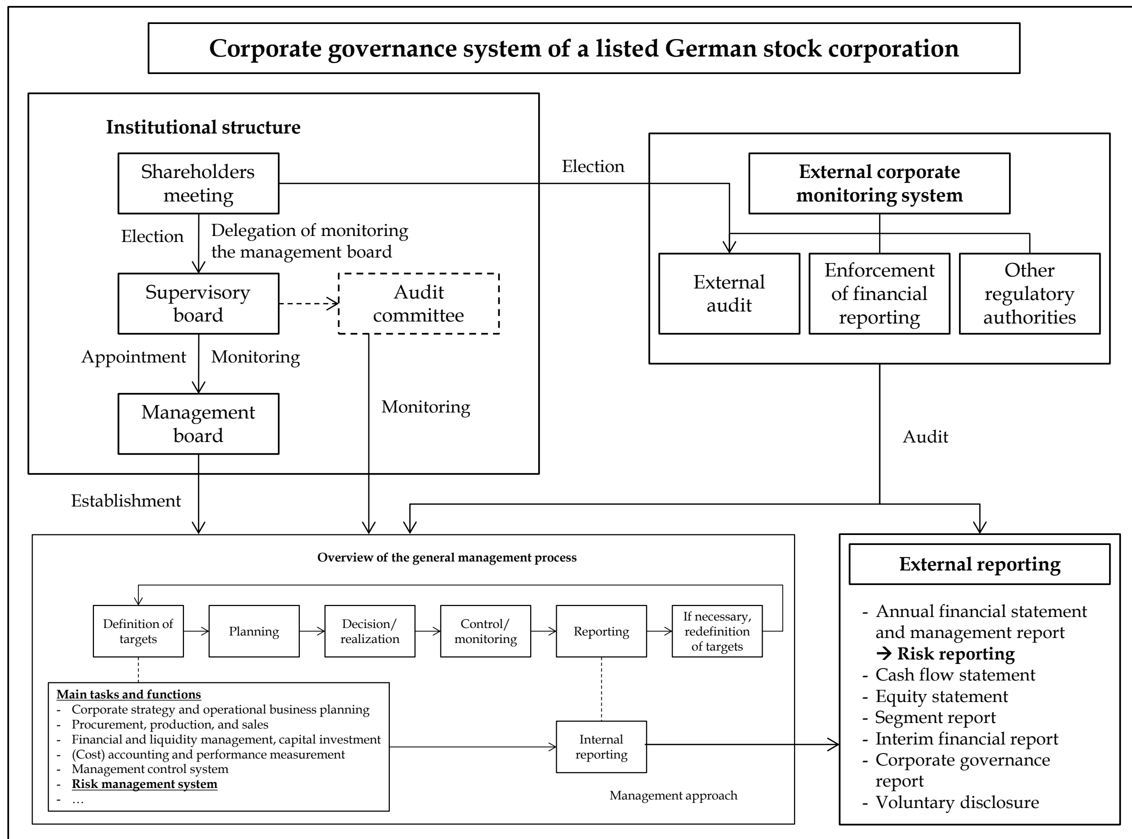
regarding the necessity of risk management and related obligations. The German two-tier system focuses primarily on the rights and responsibilities of the management board and supervisory board as well as the shareholders meeting as the main organs of a stock corporation. The shareholders meeting elects the supervisory board, which appoints and monitors the management board. These institutions have direct and implicit relations to risk management and the external corporate monitoring system. The management board is responsible for the establishment of useful management processes, which include among other things the risk management (Sec. 91(2) AktG in conjunction with Sec. 76(1) AktG). Sec. 91(2) of the AktG points out that the management board must implement suitable measures and a monitoring system to ensure early detection of developments threatening the continuation of the company. German scholars and the DCGK (para. 4.1.4) interpret this wording as an obligation to install a comprehensive risk management system (e.g., Lück 1998, p. 8–9; Freidank 2012, p. 21–24). Furthermore, it is necessary that the supervisory board monitors management (Sec. 111(1) AktG). Thus, one important task is to monitor the risk management system. The DCGK substantiates this necessity. According to para. 3.4 and para. 5.2, the management board has to inform the supervisory board regularly (during and between meetings) about all important issues relating to the firm. Among other things, risk situation assessment and risk management are mentioned explicitly. Sec. 107(3) of the AktG substantiates the necessity of monitoring the risk management system by the supervisory board. This rule deals with the possibility of implementing one or more supervisory board committees, particularly for the purposes of preparing its consultations and resolutions or for monitoring the execution of its resolutions. An audit committee is explicitly mentioned in Sec. 107(3) of the AktG. The tasks of this committee are monitoring of the accounting process, the efficiency of the internal control system, the risk management system and the internal revision system, as well as the auditor (see also DCGK, para 5.3.2). If the supervisory board has not installed an audit committee, it has to perform the aforementioned tasks itself, in particular the monitoring of the risk management system.

Secondly, this section focuses on financial reporting regulations regarding risk management. One of the management's most important activities is the preparation of financial reports, which follows the management approach (see section 2). The German accounting principles of the HGB can be characterized as general norms, which are used for each individual accounting case. Sec. 252(1)4 of the HGB requires, as one important general principle, a conservative valuation that considers all foreseeable risks. In addition to the annual financial statement (balance sheet, income statement, and notes), German firms have to prepare a management report (Sec. 289 HGB), which has to contain an assessment of the firm's current and future situation by the legal representatives of the corporation. Sec. 289(1)4 of the HGB requires in particular an assessment of the prospective development of the company with its essential opportunities and risks including the underlying assumptions. Sec. 289(2) of the HGB substantiates this necessity because the management additionally has to explain the objectives and methods of risk management. Furthermore, companies that deal in capital markets have to describe the essential characteristics of the accounting-related risk management process. In summary, a comprehensive risk report as part of the management report is necessary.

Thirdly, this section focuses on auditing and other external monitoring regulations of risk management. A company's financial reports must be audited. Risk management is simultaneously included among the external audits (Sec. 317(4) HGB in conjunction with Sec. 91(2) AktG). The shareholders meeting elects the auditor for these external audits. Furthermore, the supervisory board or the audit committee must be informed by the auditor if there are major weaknesses in the internal control and risk management system with regard to the accounting process (Sec. 171(1) AktG). Under special conditions, capital-market-oriented companies are subject to the enforcement of financial reporting by the German Financial Reporting Enforcement Panel (Deutsche Prüfstelle für Rechnungslegung) (Sec. 342b–e HGB). This affects risk management too. One main objective of this enforcement is the supervision of auditors, who are otherwise only self-monitored by a peer-review process [Sec. 57(2)1 German Auditor's Regulations (Wirtschaftsprüferordnung)].

In summary, Figure 2 (inspired by Sassen 2012, p. 327) shows the integration of risk management into the corporate governance system of a listed German stock corporation. It indicates the direct and implicit links, relationships, interactions, and dependencies between risk management and the components of corporate governance. Furthermore, it provides the basis for the following comparison with the U.S. corporate governance system.

Figure 2. Corporate governance system of a listed German stock corporation



4 Risk management as a component of the corporate governance system of a U.S. stock corporation

This section analyzes how risk management can be integrated into the U.S. corporate governance system in an analogous way. The monistically structured U.S. listed stock corporation has only two essential organs. Chapter 7 of the Model Business Corporation Act (MBCA) contains model rules for the shareholders meeting, and Chapter 8 of the MBCA deals with model rules for the board of directors (executive and non-executive). Furthermore, listed U.S. companies must comply with the rules and regulations of the Securities and Exchange Commission (SEC). The main objective of the SEC is to oversee the capital markets. All companies that wish to deal in the U.S. capital markets must follow the federal laws of the Securities Act (SA) of 1933 and the Securities Exchange Act (SEA) of 1934. Thus, the SEC has a profound significance for listed companies. The following statements describe these important rules and standards including recent reforms in relation to their relevance to risk management; the relevant norms for financial institutions will not be analyzed in detail.

Recently, two important corporate governance reforms affecting risk management among other things were implemented in the U.S. This includes the Sarbanes–Oxley Act (SOX) from 2002 as a reaction to a number of major corporate and accounting scandals (for example, Enron and WorldCom) and the Dodd–Frank Act from 2010 as a result of the financial crisis that started in 2007. The provisions of SOX were especially pertinent to companies and auditors. The main objective was a recovery of investor confidence in financial reports (Happ and Pott 2007, p. 666). The general SOX formulations were specified by the SEC. Among other aspects, the SEC had to issue rules on internal control reporting as a part of the financial report, which must be audited by a certified public accountant (CPA) (SOX 404). Here, too, risk management is part of the internal control system. Therefore, SOX had implications for the risk management of U.S. companies. The main objectives of the Dodd–Frank Act were to combat the recent financial crisis and to prevent future crises. This financial reform was implemented to improve transparency and accountability in order to stabilize financial markets, put an end to the “too big to fail” phenomenon, minimize systemic risks, and improve consumer protection (Spindler, Brandt, and Raapke 2010, p. 746). Thus, both reforms had relevance for risk management practices.

Firstly, this section focuses on the provisions of SOX 404 regarding risk management as an internal control component. The management is responsible for issuing an internal control report as part of the company’s financial statements. This report must

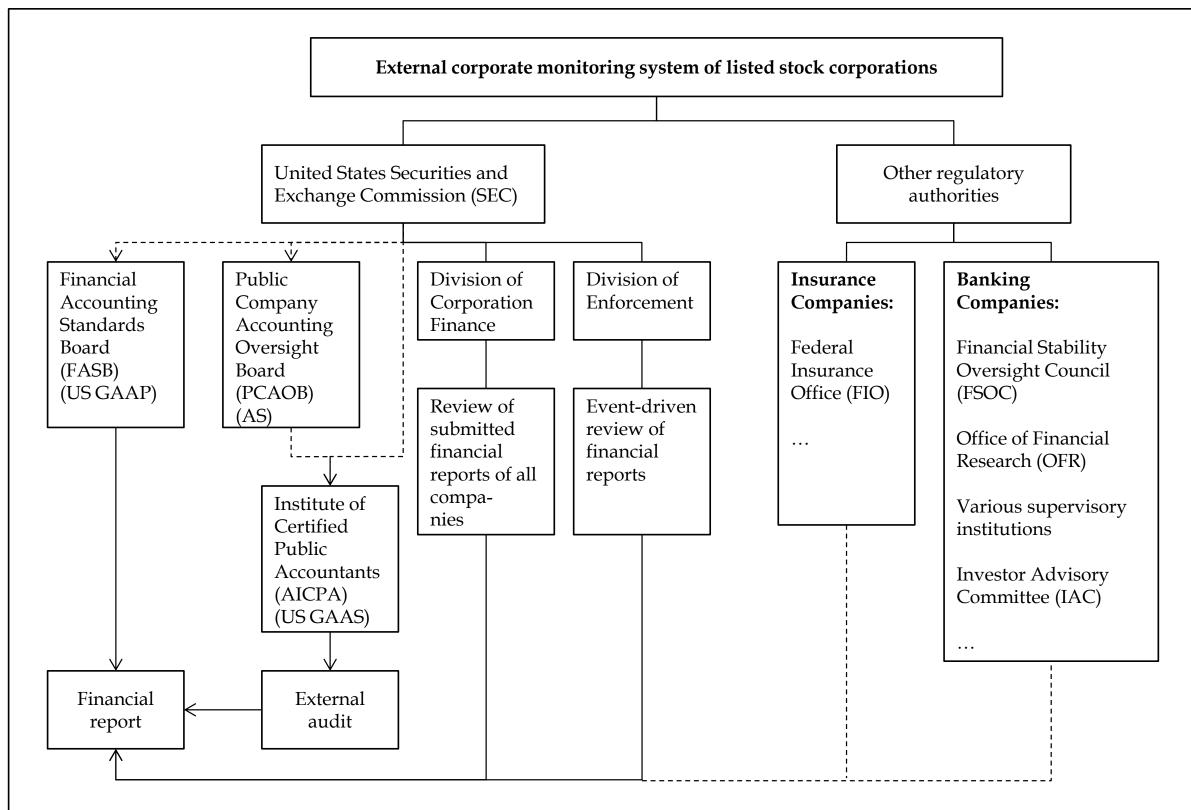
include the responsibility of management to establish and maintain adequate internal control structures and procedures regarding the financial report, and it must also contain an assessment of the effectiveness of the internal control structure and procedures. These provisions of SOX 404 were substantiated by the SEC with the "Final Rule: Management's Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports". This rule includes a definition of internal control and a description of the procedure so that management can assess its effectiveness. The SEC states that the definition of the report by the Committee of Sponsoring Organizations from the Treadway Commission (COSO report) from 1992 is appropriate. The provisions of SOX 302 strengthen the requirements of SOX 404 because the executive officer responsible (CEO/CFO) must explicitly confirm in each financial report that the provisions of SOX 404 have been applied. The internal control report must be part of the financial statements and needs to be audited by a CPA (Happ and Pott 2007, pp. 666–667). The consequence of this requirement is a need to implement internal control activities. The management is responsible for its establishment and execution and is required to create appropriate and effective internal control structures and processes for financial reporting. The COSO report (Internal Control – Integrated Framework) (COSO 1994) is an expedient approach to implement the requirements of SOX 404 because both the SEC and the Public Company Accounting Oversight Board (PCAOB) (see below) explicitly refer to it. The COSO report includes different internal control components. It requires among other things an appropriate control environment and an assessment of risk. The COSO term "risk assessment" signifies the complete risk management process, which includes identifying risks and a concrete valuation of likelihood and the financial impact of risks. The risk management process was substantiated in 2004 by the complementary "Enterprise Risk Management" framework, which requires companies to establish control activities, an adequate system of information and communication, as well as an internal monitoring system (quality control) as internal control components (COSO 2004). This framework pays special attention to the risk management process, which contains the following steps: objective setting, event identification, risk assessment, risk response, and risk communication (Happ and Pott 2007, pp. 668–669). Recently, the COSO published an updated "Internal Control – Integrated Framework" document (COSO 2013). It does not represent a paradigm shift but it does include 17 principles for the COSO components in order to complement and clarify them. Four of these principles concern risk management (COSO 2013, p. 7). In summary, in consideration of the COSO framework, SOX 404 has had an extensive regulatory effect on risk management.

Secondly, this section focuses on the SEC regulations of risk management. The SEC has special importance for the organization and structure of the external corporate monitoring system in the U.S. (Figure 3). All companies that wish to deal in the U.S. capital markets must be registered with the SEC. The strategic objectives of the SEC are above all else the provision of an effective regulatory environment and support for information-based investment decisions (Bockmann 2012, pp. 99–100, 120–121). Owing to these reasons, the SEC has extensive legislative, executive, and judicial power. The SEC's activities focus particularly on monitoring financial reporting and auditors. The SEC has also the right to set accounting standards. This right is executed only in exceptional cases because it is transferred to the Financial Accounting Standards Board (FASB). However, the SEC issues its own standards in certain circumstances, such as if there is no standard for a special accounting field, if an FASB standard is unclear and requires further interpretation, or if an FASB standard contradicts the SEC opinion. All listed companies are subject to monitoring by the SEC, and they must regularly submit documents related to their financial reporting (Bockmann 2012, pp. 100–104). The Division of Corporation Finance systematically reviews all submitted documents for form and content. The Division of Enforcement is responsible for event-related enforcement if they identify or if they receive external information about errors in the financial report. In the case of errors, they are permitted to sanction the companies under scrutiny. Thus, risk management is also subject to the enforcement of financial reporting by the SEC because this also concerns companies' reporting on internal control. According to SEA 10 and SEC Regulation S-X, financial reports of listed U.S. stock corporations must be audited because these regulations require a certified financial statement by an independent auditor. The CPA must use the United States Generally Accepted Auditing Standards (US GAAS), which are published by the American Institute of Certified Public Accountants (AICPA). There are general standards, standards of field work, standards of reporting, and statements on auditing standards (SAS). Risk management systems must be audited as well. This especially concerns the auditing of internal control processes (SOX 404). The AICPA issued its second standard of field work as a general auditing requirement: "The auditor must obtain a sufficient understanding of the entity and its environment, including its internal control, to assess the risk of material misstatement of the financial statements whether due to error or fraud, and to design the nature, timing, and extent of further audit procedures." These aspects were substantiated in particular by SAS 109 (Understanding the Entity and Its Environment and Assessing the Risks of Material

Misstatement) and SAS 115 (Communicating Internal Control Related Matters Identified in an Audit). The PCAOB was installed by SOX to oversee the external auditors and is monitored by the SEC (Happ and Pott 2007, pp. 666–667). The main tasks of the PCAOB are the registration of auditing firms, the issuing of auditing and quality standards, as well as the monitoring of auditing firms and enforcement of the implementation of SOX. The self-regulation of auditors and standard-setting by the AICPA have been limited because of the installation of the PCAOB. The PCAOB issued the Auditing Standard (AS) No. 5 on the auditing of internal control: "An Audit of Internal Control Over Financial Reporting That Is Integrated with An Audit of Financial Statements". AS No. 5 points out that the above-mentioned COSO report includes appropriate standards on the establishment and assessment of the internal control system. Additional regulatory authorities mainly oversee specific sectors (especially banking and insurance companies). These are subject to specific rules with further requirements. This paper shows only a sample of the recent reforms to illustrate the significance of these rules for risk management.

The Dodd–Frank Act installed a Financial Stability Oversight Council (FSOC) and an Office of Financial Research (OFR) to optimize financial supervision. The main objective of the FSOC and the OFR is the identification and minimization of systematic risks, which occur in large companies and complex financial statements (Spindler, Brandt, and Raapke 2010, pp. 746–747). If necessary, the FSOC can request certified reports on a company's financial situation and its risk management system. Under certain conditions, the FSOC has the option to require strict prudential regulation by the Federal Reserve System (Fed) of non-banking companies as well if these companies contain risks to the stability of the American economy. There are many different supervisory institutions in the U.S., which has led to the charter-shopping phenomenon (Spindler, Brandt, and Raapke 2010, pp. 748–749). Despite these latent conflicts, the financial reform did not include significant changes to the composition of supervisory institutions. Instead, additional disclosure requirements were implemented to reduce potential conflicts of interest. Consequently, the Dodd–Frank Act installed an Investor Advisory Committee (IAC). The main objective of the IAC is the identification and minimization of supervisory gaps in cooperation with the SEC. Until the adoption of the Dodd–Frank Act, insurance companies only had to follow a prudential regulation that was determined by each U.S. federal state. Now the Federal Insurance Office (FIO) has been installed to coordinate the supervisory work in the U.S. (Hünermann and Dietrich 2010, p. 360).

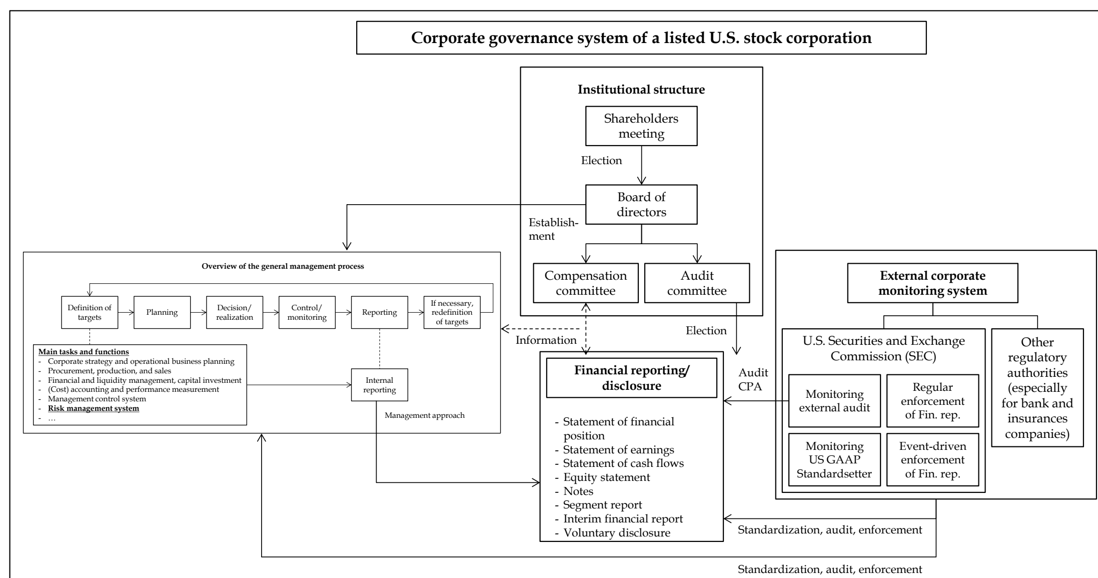
Figure 3. External corporate monitoring system of listed stock corporations



Thirdly, this section focuses on financial reporting regulations of risk management. Listed stock corporations must apply the United States Generally Accepted Accounting Principles (US GAAP) to their financial reporting, although this requirement is not directly stated by law. The SEC requires listed stock corporations to provide financial statements, which must be audited by a CPA. The CPA must follow the US GAAS, issued by the AICPA (SEC Regulation S-X). It is the US GAAS that requires companies to apply US GAAP, issued by the FASB. In the U.S., financial statements contain a statement of financial position, statement of earnings, statements of cash flows, equity statement, and notes (SEC Regulation S-X, SEC Regulation S-K). Furthermore, there are segment reports and interim financial reports. The U.S. accounting standards contain various requirements for risk management that are not discussed in detail, but Xu, Grove, and Schaberl (2013) have highlighted that risk management has taken on a new priority because the SEC now requires more disclosures on risk management and corporate governance, especially on the role of the board of directors in risk management oversight (p. 104).

Figure 4 shows the corporate governance system of a U.S. listed stock corporation. It is organized on the basis of the institutional structure. The shareholders meeting elects the board of directors, which can form various committees (MBCA 8.25). There are individual rules for audit committees (SEA 10a) and compensation committees (SEA 10c). In addition, it is possible to form other company-specific committees. The audit committee is responsible for the election of the auditor and therefore has corresponding links to risk management. The board of directors is also responsible for the establishment of a useful management process, which includes risk management as an internal control component (SOX 404). Owing to the management approach, management is responsible for preparing the financial reports, which are audited and overseen by the external corporate monitoring system. The risk management in turn is part of the auditing and monitoring activities of the external corporate monitoring system, which is shaped by the strong role of the SEC.

Figure 4. Corporate governance system of a listed U.S. stock corporation



5 Conclusions

There are many corporate governance regulations that are relevant to the risk management of listed stock corporations in Germany as well as in the U.S. This applies to the management process, the management-approach-oriented financial reporting, and the external monitoring system. There are norms that regulate risk management directly both in Germany and the United States. Sec. 91(2) of the AktG plays a major role in Germany, and SOX 404 plays a major role in the U.S.

In summary, the requirement of risk management is standardized in both countries. The recent corporate governance reforms in both countries focus increasingly, directly or indirectly, on an optimization of risk management. Thus, this paper has outlined the integration of risk management into the corporate governance system of listed stock corporations for both countries. Furthermore, it has pointed out interactions and dependencies between the different components of corporate governance.

Table 1 represents a tabular comparison of the essential aspects of the systemic integration of risk management into the corporate governance systems of listed stock corporations in Germany and the U.S.

Table 1. Tabular comparison of the corporate governance system of a German and U.S. listed stock corporation

	Germany	Regulation level	Points	United States	Regulation level	Points
Institutional structure	Dual (two-tier) system: separation between management and supervisory board.			Monistic (one-tier) system: no separation between management and supervisory board.		
	There are further consequences or deviations because of the general distinction between the institutional structures (for example, the responsibility for electing the auditor).					
Risk management	Regulated by law, but not specified (Sec. 91(2) AktG). Therefore, the management has to interpret how the risk management should be designed.			Regulated quasi-legally (COSO I & II) and highly specified (internal control under SOX 404). Thus, risk management is highly regulated.		
- **Implementation**	- Early risk detection (Sec. 91(2) AktG) as one risk management function. - Risk management (DCGK, para. 4.1.4).	Mandatory Implicit mandatory	2.5 of 5.0	Risk management as internal control component (SOX 404).	Mandatory	5.0 of 5.0
- **Process**	-	-	0.0 of 5.0	COSO process: - Objective setting. - Event identification. - Risk assessment. - Risk response. - Risk communication.	Implicit mandatory	2.5 of 5.0
Financial reporting	For listed companies regulated by German GAAP (HGB), which tend towards the management approach.			Regulated by the US GAAP standards issued by the FASB, which tend towards the management approach and are strongly influenced by the SEC.		
- **Accounting**	HGB: General norms for each individual case, which requires a conservative valuation considering all foreseeable risks (Sec. 252(1)4 HGB).	Mandatory	1.0 of 1.0	US GAAP: Individual standards for different cases that sometimes affect risks.	Mandatory	0.5 of 1.0
- **Reporting**	Necessity of a comprehensive risk report as part of the management report (Sec. 289 HGB)	Mandatory	2.0 of 2.0	Risk reporting depending on the individual requirements of the US GAAP.	Mandatory	1.0 of 2.0
External corporate monitoring system	In summary, the external corporate monitoring system of U.S. listed stock corporations seems to be more strongly regulated than the German system because of the strong and coordinating role of the SEC, even though the underlying regulations usually have only a quasi-legal character.					
- **External audit**	Basically identical auditing requirements. In terms of risk management, an audit of the management-approach-oriented financial reporting as well as risk management or internal control are necessary.					
	Risk-oriented audit approach.	Mandatory		Risk-oriented audit approach.	Mandatory	
- **Enforcement of auditors**	Self-regulation of auditors (peer review).			Additional auditing standards issued by the PCAOB (also for internal control) and enforcement of auditors by the PCAOB		
- **Enforcement of financial reporting**	Regular audits in samples and event-related audits (including aspects related to risk management).		1.0 of 1.0	All submitted financial reports are systematically analyzed formally and materially, also event-related audits (including aspects related to risk management).		1.0 of 1.0
- **Other regulatory authorities**	There are further specific risk management-related requirements for banking and insurance companies in Germany and the U.S., which are not analyzed in detail here.					
Regulation approach	More strongly legally oriented and only a few supervisory authorities.		**Sum: 6.5 (14.0)**	Strong role of the SEC and to a greater extent regulated by quasi-legal standards.		**Sum: 10.0 (14.0)**

There are differences and commonalities between the integration of risk management into the corporate governance system in these countries. To visually represent these differences and commonalities, Table 1 depicts a semi-quantitative scoring. Direct regulations of the implementation and the process of risk management are weighted higher (with five points each) than the reporting (three points) and the external monitoring (one point) requirements for risk management. In cases of mandatory rules, the categories received all possible points, and in cases of implicit requirements they received only half the number of points. The nature of this scoring is obviously subjective, but it nevertheless seems that the U.S. corporate governance system is more strongly regulated than its German counterpart because there are more detailed requirements for the risk management process, even though the character of the underlying regulations is usually only quasi-legal. Thus, the seemingly more liberal system of non-binding standards in the U.S. has greater significance for the regulation of risk management than in Germany. This can be explained by the strong role of the SEC, which has a high influence on various standard setters on the one hand and a strong role in monitoring regulated companies on the other.

Regarding future research, it is worth mentioning that comparisons can only state the differences and commonalities between the systems. It is not yet possible to determine whether a high or low level of regulation is appropriate. Thus, one next research step could be to integrate the benefits and costs of the regulation of risk management into a systematic regulatory model that would determine a regulatory theoretical optimum (Freidank and Sassen 2012, pp. 161–189). An alternative next research step could be an empirical investigation of the extent to which risk management systems and processes have been implemented in order to draw conclusions on the different national levels of implementation and regulation.

References

1. Acharya, V.A., Myers, S.C. & Rajan, R.G. (2011). The internal governance of firms. The Journal of Finance, 66, pp. 689–720.
2. Bebchuk, L.A. & Weisbach, M.S. (2010). The state of corporate governance research. The Review of Financial Studies, 23, pp. 939–961.
3. Bockmann, R. (2012). Internationale Koordinierung nationaler Enforcement-Aktivitäten. Eine kritische Analyse unter besonderer Berücksichtigung der Deutschen Prüfstelle für Rechnungslegung. Wiesbaden.
4. Brezeanu, P., Al Essawi, M.S., Poanta, D. & Badea, L. (2011). Does corporate governance impact risk management system? Theoretical and Applied Economics, 18, No. 4, pp. 49–64.
5. Cadbury Commission (1992), Report of the Committee on the Financial Aspects of Corporate Governance. London.
6. COSO (Committee of Sponsoring Organizations of the Treadway Commission) (1994). Internal Control – Integrated Framework. Jersey City & New Jersey.
7. COSO (Committee of Sponsoring Organizations of the Treadway Commission) (2004). Enterprise Risk Management – Integrated Framework. Jersey City & New Jersey.
8. COSO (Committee of Sponsoring Organizations of the Treadway Commission) (2013), Internal Control – Integrated Framework Executive Summary (May 14, 2013), available under: http://www.coso.org.
9. Daelen, M. van & Ven, A.C.N. van de (2010). Introducing risk management. In Daelen, M. van & Elst, C. van der (ed), Risk Management and Corporate Governance. Interconnections in Law, Accounting and Tax. Cheltenham & Northhampton, pp. 1–6
10. DCGK (Deutscher Corporate Governance Kodex). German Corporate Governance Code (latest version: May 13, 2013), available at http://www.corporate-governance-code.de.
11. Fama, E. F. & Jensen, M. C. (1983). Separation of Ownership and Control. Journal of Law & Economics, 26, pp. 301–325.
12. Freidank, C.-Chr. (2012). Unternehmensüberwachung. Die Grundlagen betriebswirtschaftlicher Kontrolle, Prüfung und Aufsicht. Munich.
13. Freidank, C.-Chr. & Sassen, R. (2012). Regulierungstheoretischer Ansatz des Controllings: Notwendigkeit einer Weiterentwicklung von Unternehmensführung und -überwachung. In Freidank, C.-Chr. & Velte, P. (ed), Corporate Governance, Abschlussprüfung und Compliance. Neue Entwicklungen aus nationaler und internationaler Sicht. Berlin, pp. 161–189.
14. Froot, K., Scharfstein, D. & Stein, J.C. (1993). Risk management: coordinating corporate investment and financing policies. The Journal of Finance, 48, pp. 1629–1658.
15. Günther, T. (2013). Conceptualisations of ‘controlling’ in German-speaking countries: analysis and comparison with Anglo-American management control frameworks. Journal of Management Control, 23, pp. 269–290.
16. Happ, D. & Pott, C. (2007). Auswirkungen des Sarbanes–Oxley Act Section 404: Kosten und Nutzen für europäische Unternehmen. KoR - Zeitschrift für internationale und kapitalmarktorientierte Rechnungslegung, 7, pp. 666–672.
17. Hopt, K.J. (2011). Vergleichende Corporate Governance. Forschung und internationale Regulierung. Zeitschrift für das gesamte Handels- und Wirtschaftsrecht, 175, pp. 444–526.
18. Hünermann, R. & Dietrich, T. (2010). Aktuelle Rechtsentwicklungen in den USA – Einflussnahme auf europäische Unternehmen. Corporate Finance Law, 1, pp. 357–363.
19. Lück, W. (1998). Elemente eines Risiko-Managementsystems: Die Notwendigkeit eines Risiko-Managementsystems durch den Entwurf eines Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG). Der Betrieb, 51, pp. 8–14.
20. Pirson, M. & Turnbull, S. (2011). Corporate governance, risk management, and the financial crisis:

An information processing view. Corporate Governance: An International Review, 19, pp. 450–470.
21. Quon, T.K., Zéghal, D. & Maingot, M. (2012). Enterprise risk management and business performance during the financial and economic crises. Problems and Perspectives in Management, 10, pp. 95–103.
22. Rappaport, A. (1986). Creating Shareholder Value, The New Standard for Business Performance, New York & London.
23. Ryan, S.G. (2012). Risk reporting quality: implications of academic research for financial reporting policy. Accounting and Business Research, 42, pp. 295–324
24. Sarens, G. & Christopher, J. (2010). The association between corporate governance guidelines and risk management and internal control practices. Evidence from a comparative study. Managerial Auditing Journal, 25, pp. 288–308.
25. Sassen, R. (2012). Integration des Controllings in das Corporate Governance-System einer Aktiengesellschaft. Zeitschrift Controlling, 24, pp. 323–329.
26. Shleifer, A. & Vishny, R.W. (1997). A survey of corporate governance. The Journal of Finance, 52, pp. 737–783.
27. Spindler, G., Brandt, K. & Raapke, J. (2010). Finanzmarktreform in den USA. Der neue Dodd-Frank Wall Street Reform and Consumer Protection Act. Recht der internationalen Wirtschaft, 56, pp. 746–753.
28. Tao, N.B. & Hutchinson, M. (2013). Corporate governance and risk management: the role of risk management and compensation committees. Journal of Contemporary Accounting & Economics, 9, pp. 83–99.
29. Velte, P. (2008). Management approach. Journal of Management Control, 19, pp. 133–138.
30. Wöhe, G. & Döring, U. (2013). Einführung in die Allgemeine Betriebswirtschaftslehre, 25th ed., Munich.
31. Xu, T., Grove, H. & Schaberl, P. (2013), Corporate governance: A risk management approach. Corporate Ownership & Control, 10, pp. 104–113.