Frank Romeike (Hrsg.)

Rechtliche Grundlagen des Risikomanagements

Haftungs- und Strafvermeidung für Corporate Compliance

ESV
ERICH SCHMIDT VERLAG

Rechtliche Grundlagen des Risikomanagements

Haftungs- und Strafvermeidung für Corporate Compliance

Herausgegeben von

Frank Romeike

Mit Beiträgen von

Dr. Jens-Hinrich Binder,
Dr. Jörg Borchert,
Dr. Jutta Jessenberger,
Dr. Manuel Lorenz,
Dr. Thomas Münzenberg,
Frank Romeike,
Prof. Dr. Hans-Peter Schwintowski,
Dr. Peter Winter,
Gundolf Zimmermann

ERICH SCHMIDT VERLAG

Bibliografische Information der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation
in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten
sind im Internet über dnb.ddb.de abrufbar.

Weitere Informationen zu diesem Titel finden Sie im Internet unter
ESV.info/978 3 503 10647 9

ISBN 978 3 503 10647 9

Dieses Papier erfüllt die Frankfurter Forderungen
der Deutschen Bibliothek und der Gesellschaft für das Buch
bezüglich der Alterungsbeständigkeit und entspricht
sowohl den strengen Bestimmungen der US Norm Ansi/Niso
Z 39.48-1992 als auch der ISO-Norm 9706.

Satz: Jung Crossmedia, Lahnau
Druck und buchbinderische Verarbeitung: Hubert & Co., Göttingen

Vorwort

Jean-Baptiste Poquelin (besser bekannt als Molière, 1622–73) erkannte bereits vor einigen Jahrhunderten: „Wir sind nicht nur für das verantwortlich, was wir tun, sondern auch für das, was wir nicht tun."

Ein Urteil des Landgerichts München vom 5. April 2007 (Az.: 5 HK O 15964/06) unterstreicht noch einmal die Relevanz eines funktionierenden Risikomanagement-Systems sowie die adäquate Dokumentation der Risikomanagement-Prozesse und -Verantwortlichkeiten. So mangelte es in diesem speziellen Fall eines Münchener Unternehmens unter anderem an der schriftlichen Dokumentation des Risikomanagements. Die Richter wiesen in diesem Kontext darauf hin, dass ein Vorstand geeignete Risikomanagement-Maßnahmen zu treffen hat, insbesondere ein Überwachungssystem einrichten sollte, damit eine den Fortbestand der Gesellschaft gefährdende Entwicklung früh erkannt werden könne. Der hier heranzuziehende § 91 Absatz 2 Aktiengesetz ist vom Gesetzgeber deshalb eingeführt worden, um angesichts offensichtlich fehlender Risikomanagementsysteme in den Unternehmen durch eine ausdrückliche Regelung diese Verpflichtung besonders hervorzuheben.

Das Risikomanagement soll in diesem Kontext nicht nur die technischen Bedrohungen erkennen, sondern auch die rechtlichen Auswirkungen einzelner Bedrohungen und die Haftungsrisiken berücksichtigen. Hierzu ist erforderlich, die für das jeweilige Unternehmen und die jeweilige Branche einschlägigen gesetzlichen und regulatorischen Anforderungen zu evaluieren, ebenso das Maß ihrer tatsächlichen Erfüllung im Unternehmen.

Die Münchener Richter rügten in ihrem Urteil auch die Arbeit der Wirtschaftsprüfer. Denn bei der Prüfung des Jahresabschlusses müssen sie auch das Überwachungssystem zur Risikofrüherkennung untersuchen, das der Vorstand nach § 91 Absatz 2 Aktiengesetz einrichten muss. Dazu stand im Bericht: „Der Vorstand hat (...) ein Überwachungssystem eingerichtet, um bestandsgefährdende Entwicklungen frühzeitig zu erkennen. Unsere Prüfung hat ergeben, dass für das vom Vorstand eingerichtetes Überwachungssystem keine formelle Dokumentation vorliegt. Somit war eine Funktions- und Systemprüfung nicht möglich."

Jedoch hatten sich die Wirtschaftsprüfer „durch Befragung des Vorstandes" davon überzeugt, dass die Gesellschaft über ein informelles Risikofrüherkennungssystem verfügt. „Wir haben den Vorstand auf seine Pflicht zur Dokumentation des Risikofrüherkennungssystems hingewiesen." Diese Passage fehlte jedoch in einem korrigierten Jahresabschluss der Gesellschaft. Der Bericht des Aufsichtsrats enthält ebenfalls keinen Hinweis auf das mangelhafte Risikomanagement.

Die Richter sahen nun einen schwerwiegenden Rechtsverstoß in der fehlenden Dokumentation des Risikofrüherkennungssystems.

aus: Romeike (Hrsg.), Rechtliche Grundlagen des Risikomanagements.

Bereits in älteren Urteilen hatten Gerichte die Verantwortung des Vorstands zum Aufbau eines Risikofrüherkennungs- sowie Risikoüberwachungssystems angemahnt (siehe beispielsweise Verwaltungsgericht Frankfurt am Main, RiskNET-News vom 7.9.2004, www.risknet.de).

In dem Urteil vom 8. Juli 2004 entschied die für Versicherungsaufsichtsrecht zuständige Kammer des Verwaltungsgerichts Frankfurt am Main über die Klage eines Vorstandsmitglieds, der sich gegen die Rechtmäßigkeit zweier Verfügungen der BaFin (Bundesanstalt für Finanzdienstleistungsaufsicht) wandte. Mit diesen Verfügungen hatte die BaFin vom Aufsichtsrat des Versicherers verlangt, den Kläger als Mitglied des Vorstandes abzuberufen. Zwischen dem 10. und dem 14. Juni 2002 fand bei dem Versicherer eine örtliche Prüfung seitens der BaFin statt. Diese Prüfung ergab unter anderem, dass bei dem Versicherer die stillen Lasten aus Aktienengagement in mehreren Investmentfonds auf etwa 93 Mio. Euro angewachsen waren, die sich zum Jahresende 2001 auf etwa 55 Mio. Euro und Mitte 2001 auf etwa 26 Mio. Euro belaufen hatten. Im Juni 2002 kam es auf Anordnung der BaFin daraufhin zur Einsetzung eines Sonderbeauftragten für den Vorstand des Versicherers.

Mit Bescheid vom 12. Dezember 2002 verlangte die BaFin schließlich vom Aufsichtsrat der zwei Versicherungsunternehmen, in denen der Kläger Vorstandsmitglied war, ihn als Mitglied des Vorstandes abzuberufen. Diesem Verlangen folgten die jeweiligen Aufsichtsräte. Die BaFin begründete ihr Vorgehen damit, dass der Kläger nicht mehr den Anforderungen des Versicherungsaufsichtsgesetzes bzgl. der fachlichen Eignung von Geschäftsleitern von Versicherungsunternehmen genüge. Bei dem Versicherer sei im Hinblick auf die stillen Lasten aus Aktienengagements in mehreren Fonds eine existenzgefährdende Lage eingetreten. Diese finanzielle Schieflage sei maßgeblich auch auf fachliche Mängel im Bereich Controlling zurückzuführen. Bestimmte Missstände seien maßgeblich dem Kläger als für das Controlling zuständigen Vorstandsmitglied anzulasten. Vor dem Hintergrund dieser Mängel sei das Abberufungsverlangen notwendig, um Belange der Versicherten zu wahren.

Der Kläger hielt dem entgegen, er habe in der kritischen Phase der Unternehmen seine Verantwortung als Ressortvorstand Controlling durchgängig aktiv wahrgenommen. Er habe sich zum Beispiel wiederholt mit eindeutigen Warnungen gegenüber Aufsichtsrat und Vorstand des Versicherers zu Wort gemeldet. Das Ressortcontrolling habe dem Vorstand regelmäßig monatlich über die Entwicklung der Zeitwerte und der stillen Lasten berichtet. Die Installation eines Risikosystems sowie eines Risikolimitsystems sei der Beklagten zugesichert worden. Für den Bereich Kapitalanlage sei ein anderes Vorstandsmitglied zuständig gewesen. Dieses habe dem Kläger nach bestimmten Vorgaben berichten sollen. Eine solche Informationsmitteilung seitens des Bereichs Kapitalanlagen sei jedoch zu keinem Zeitpunkt erfolgt. Es habe für ihn aber auch keinerlei Anzeichen dafür gegeben, dass die Vorstände für den Bereich Kapitalanlage oder den Bereich Revision ihre erhaltenen Aufträge nicht ausführen würden.

Versicherungsunternehmen dürfen ihren Geschäftsbetrieb nur mit einer Erlaubnis der BaFin als Aufsichtsbehörde aufnehmen (§ 5 VAG). Diese Erlaubnis ist unter anderem dann zu versagen, wenn Tatsachen vorliegen, die den Schluss darauf zulassen („die die Annahme rechtfertigen"), dass der Betriebsinhaber oder – bei juris-

tischen Personen – ein gesetzlicher oder satzungsmäßiger Vertreter nicht zuverlässig ist oder aus anderen Gründen nicht den im Interesse einer soliden und umsichtigen Führung des Erstversicherungsunternehmens zu stellenden Ansprüchen genügt. Unter den selben Voraussetzungen kann die BaFin auch ein Abberufungsverlangen stellen, wenn ihr nachträglich solche Tatsachen bekannt werden (§ 87 Abs. 6 VAG). Nach Auffassung des Verwaltungsgerichts hat die BaFin auf dieser Gesetzesgrundlage rechtmäßig gehandelt, so dass der Kläger nicht in seinen Rechten verletzt ist.

Das Gericht stellte des Weiteren klar, dass der Vorstand in seiner Gesamtverantwortung ein Risikofrüherkennungs- und -überwachungssystem einzurichten hat, damit eine den Fortbestand der Gesellschaft gefährdende Entwicklung früh erkannt werden könne. In diesem Kontext wies das Gericht auch darauf hin, dass bereits vor Inkrafttreten des hier entsprechend anwendbaren § 91 Abs. 2 Aktiengesetz entsprechende Verpflichtungen zur Schaffung angemessener interner Kontrollverfahren bestanden (§ 81 Abs. 1 Satz 5 Versicherungsaufsichtsgesetz und § 25 a Kreditwesengesetz). Mit Einführung des § 91 Abs. 2 Aktiengesetz im Jahre 1998 habe der Gesetzgeber die Verpflichtung der Geschäftsleitung hervorheben wollen, Risikofrüherkennungs- sowie Risikoüberwachungssysteme in den Unternehmen einzurichten, um Entwicklungen vorzubeugen, die den Fortbestand der Gesellschaft gefährden könnten. Der Gesetzgeber habe nämlich erkannt, dass die Ursache von Fehlentwicklungen vielmals an einer mangelhaften Risikoeinschätzung der Unternehmensleitungen gelegen habe, so dass nicht frühzeitig auf drohende Schieflagen der Unternehmen habe reagiert werden können.

In der vorliegenden Publikation werden die gesetzlichen Grundlagen des Risikomanagements zusammenfassend dargestellt. Hierbei handelt es sich entweder um zwingende Rechtsvorschriften (§ 91 Absatz 2 AktG, § 93 Absatz 1 Satz 1 AktG etc.) oder um „Codes of Best Practise" (COSO Report, Cadbury Committee etc.). Ausgangspunkt ist ein branchenübergreifender Überblick über den gesetzlichen Rahmen.

Dr. Manuel Lorenz skizziert in seinem Einführungsbeitrag die gesetzlichen Grundlagen des Risikomanagements im nationalen Kontext. Einen ganz wesentlichen Beitrag zur Fortentwicklung Deutscher Corporate Governance lieferte der deutsche Gesetzgeber bereits mit der Verabschiedung des KonTraG („Gesetz zur Kontrolle und Transparenz im Unternehmensbereich"). Das KonTraG verpflichtet seit 1. Mai 1998 Vorstände börsennotierter Unternehmen in Deutschland explizit zur Einrichtung eines Überwachungssystems, um Risiken frühzeitig zu erkennen. Der Beitrag „Anforderungen des Deutschen Corporate Governance Kodexes an das Risikomanagement" (**Frank Romeike**) liefert einen Überblick über das Ergebnis der Diskussion um „gute Unternehmensführung" in Deutschland. **Dr. Peter Winter** gibt in seinem Beitrag einen Überblick über Standards im Risikomanagement. Mit den straf- und zivilrechtlichen Auswirkungen auf die Haftung der Unternehmensleitung setzt sich **Dr. Thomas Münzenberg** auseinander.

Der zweite Teil des Buches setzt sich mit den branchenspezifischen Rechtsgrundlagen des Risikomanagements auseinander. **Dr. Jens-Hinrich Binder** stellt in seinem Beitrag die rechtlichen Grundlagen des Risikomanagements in Banken und Finanzdienstleistungsinstituten dar. So stellt insbesondere der „New Basel Capital Accord" (besser bekannt unter dem Begriff „Basel II") höhere Anforderungen an das Con-

trolling und Risikomanagement von Banken. **Prof. Dr. Hans-Peter Schwintowski** skizziert in seinem Beitrag die rechtlichen Grundlagen des Risikomanagements in Versicherungsunternehmen. So müssen Versicherer zukünftig ihren Eigenkapitalbedarf nach EU-einheitlichen Vorgaben (Solvency II) wesentlich mehr als bisher an den eingegangen Risiken ausrichten. In diesem Zusammenhang sollen auch die Aufsichtsregeln harmonisiert werden. Anfang Juli 2007 wurde die Solvency-II-Rahmenrichtlinie von der EU-Kommission verabschiedet. **Dr. Jutta Jessenberger** und **Gundolf Zimmermann** konzentrieren sich in ihren Ausführungen auf die spezifischen rechtlichen Grundlagen des Risikomanagements im internationalen Industriekonzern. Schließlich skizziert **Dr. Jörg Borchert** die rechtlichen Grundlagen des Risikomanagements im Energiemarkt/-handel.

An dieser Stelle möchte ich die Gelegenheit nutzen, um denjenigen Personen zu danken, die zum Gelingen des Buches beigetragen haben. Als Herausgeber bedanke ich mich bei allen mitwirkenden Autoren für Ihre spontane und bleibende Bereitschaft zur Mitarbeit. Ein besonderer Dank gilt Frau Dr. Anette Köcher, die durch ihr theoretisches und praktisches Wissen im Bereich des Risikomanagements stets als kompetente und kritische Gesprächspartnerin zur Verfügung stand. Darüber hinaus gilt mein Dank Herrn Dr. Joachim Schmidt, mit dem ich gemeinsam die Idee zu diesem Buch hatte und der das Projekt über die vergangenen Monate verlagsseitig begleitet hat.

Wir würden uns sehr freuen, wenn Sie aus dem Buch viele Anregungen für die Entwicklung oder Weiterentwicklung Ihrer vorhandenen Managementsysteme finden, die den Umgang mit den unvermeidlichen Risiken jeglicher unternehmerischen Tätigkeit verbessern. Kritik und Wünsche nehmen wir gerne auf: Schreiben Sie eine E-Mail an buch@risknet.de.

Oberaudorf am Kaisergebirge im August 2007
Frank Romeike

Inhaltsverzeichnis

1. Einleitung

Die Organe einer Kapitalgesellschaft mit Sitz in Deutschland sind grundsätzlich verpflichtet, ein Risikomanagementsystem einzurichten und zu betreiben. Diese Verpflichtung beruht auf verschiedenen rechtlichen Grundlagen, aus denen sich auch Mindestanforderungen für die Ausgestaltung eines solchen Systems ergeben.

In den neunziger Jahren ist eine kontroverse Diskussion um die Einrichtung von Risikomanagementsystemen in deutschen Unternehmen ausgebrochen, als der deutsche Gesetzgeber als zentrales Element des Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) durch den neu geschaffenen § 91 Abs. 2 AktG für Aktiengesellschaften die Pflicht zur Schaffung eines Überwachungssystems für bestandsgefährdende Entwicklungen gesetzlich verankert hat. Weitere Normen des KonTraG beschäftigen sich mit der Risikoberichterstattung im Jahresabschluss und der Überprüfung durch die Abschlussprüfer und liefern damit Anhaltspunkte für die Ausgestaltung der Unternehmensorganisation. Gesetzgeberisches Motiv für das KonTraG waren Schwächen und Verhaltensfehlsteuerungen im deutschen System der Unternehmenskontrolle, die in der Vergangenheit zu Aufsehen erregenden Unternehmenskrisen geführt haben. Infolge von negativen Unternehmensentwicklungen wie etwa bei der Metallgesellschaft, der Bremer Vulkan oder dem Komplex Balsam/Procedo rückte die Frage in den Vordergrund, inwieweit diese Entwicklungen auf das Fehlen angemessener Risikomanagement- und Controllingsysteme in den jeweiligen Unternehmen zurückzuführen waren und unter Umständen hätten verhindert werden können. Dabei sind insbesondere Großunternehmen von den Neuregelungen betroffen, bei denen die Gefahr besteht, dass Risiken auf nachgeordneten Entscheidungsebenen von den Unternehmensleitungen nicht wahrgenommen werden. Eine grenzüberschreitende Unternehmenstätigkeit kann die Leitung zusätzlich erschweren.

Das KonTraG ist freilich nicht die einzige Rechtsquelle für das Risikomanagement. Gesetzgeber haben auch international auf Unternehmenszusammenbrüche und Bilanzskandale reagiert. Nachstehend werden neben Vorschriften des deutschen Rechts auch europäische und US-amerikanische Rechtsquellen angesprochen, die sich unmittelbar oder mittelbar mit der Behandlung von Risiken beschäftigen und die eine Ausstrahlungswirkung für die Auslegung und Anwendung bereits bestehender und durch das KonTraG neu eingeführter Vorschriften haben.

Es stellen sich verschiedene Fragen in Bezug auf eine „best practice“ der Unternehmensorganisation im Umgang mit Risiken, um einerseits eine positive Unternehmensentwicklung zu ermöglichen und andererseits die Verantwortlichen keinen Haftungsrisiken auszusetzen.

Entsprechende Ansätze werden nachstehend kurz vorgestellt. Abschließend wird dargestellt, wie Haftungsregelungen die Ausgestaltung und Anwendung eines Risikomanagementsystems beeinflussen, und welche Rolle der Aufsichtsrat dabei spielt.

aus: Romeike (Hrsg.), Rechtliche Grundlagen des Risikomanagements.

2. Das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)

2.1 § 91 Abs. 2 AktG

§ 91 Abs. 2 AktG bestimmt:

„Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand des Unternehmens gefährdende Entwicklungen früh erkannt werden."

Schon die Gesetzesbegründung[1] weist darauf hin, dass mit dieser Vorschrift keine neue Leitungsaufgabe für den Vorstand geschaffen worden ist, sondern lediglich eine Aufgabe besonders hervorgehoben werden sollte.

§ 91 Abs. 2 AktG hat zwar keine Entsprechung im GmbH- oder Personengesellschaftsrecht, aber die Vorschrift hat ausweislich der Gesetzesbegründung eine „Ausstrahlungswirkung" auf andere Gesellschaftsformen. Die Intensität dieser Ausstrahlungswirkung ist von der Größe und der Komplexität der jeweiligen Unternehmensstruktur abhängig.[2]

Auffällig an der Vorschrift ist, dass keine ausdrückliche Pflicht begründet wird, ein umfassendes Risikomanagementsystem einzurichten. Angesprochen wird allenfalls eine Komponente eines Risikomanagementsystems, nämlich die Einrichtung eines Überwachungssystems zur Früherkennung von bestandsgefährdenden Entwicklungen. Nicht einmal der Begriff „Risiken" wird in § 91 Abs. 2 AktG verwendet, sondern nur der Begriff „Entwicklungen".[3] Auch wie der Vorstand mit erkannten bestandsgefährdenden Risiken oder Entwicklungen umgeht, wird im Gesetz nicht explizit geregelt. Nach Einschätzung des Gesetzgebers gehören zu den Entwicklungen, die den Fortbestand der Gesellschaft i. S. d. § 91 Abs. 2 AktG gefährden können, insbesondere risikobehaftete Geschäfte, Unrichtigkeiten der Rechnungslegung und Verstöße gegen gesetzliche Vorschriften, die sich auf die Vermögens-, Finanz- und Ertragslage der Gesellschaft oder des Konzerns wesentlich auswirken.[4]

Sowohl in der juristischen als auch in der betriebswirtschaftlichen Literatur und in der Prüfungspraxis wird lebhaft über die Anforderungen diskutiert, die im Einzelnen an die einzurichtende Organisation der Risikoanalyse, Risikoquantifizierung und letztendlich ein Risikomanagement zu stellen sind.

In der Literatur herrschen beträchtliche Meinungsunterschiede zu der Frage, ob sich aus § 91 Abs. 2 AktG bereits die Pflicht zur Einrichtung eines vollwertigen Risikomanagementsystems ergibt.[5] Es lassen sich drei Auffassungen unterscheiden, wobei sich in erster Linie das juristische Schrifttum und die Betriebswirtschaftslehre

1 BT-Drucks. 13/9712, S. 15.

2 Vgl. Altmeppen, Die Auswirkungen des KonTraG auf die GmbH, ZGR 1999, S. 301f.

3 Hinweis auch bei Seibert, Die Entstehung des § 91 Abs. 2 AktG im KontraG, in Festschrift für Bezzenberger, S. 437, wonach fortlaufende Entwicklungen und nicht abstrakte oder latente Risiken gemeint seien.

4 Vgl. BT-Drucks. 13/9712, S. 15.

5 Dagegen: Seibert, Die Entstehung des § 91 Abs. 2 AktG im KonTraG, in Festschrift für Bezzenberger 2000, S. 437, Hüffer, Aktiengesetz, 7. Auflage 2006, § 91 Rn. 9.

bzw. Prüfungspraxis gegenüberstehen. Eine dritte Meinung nimmt einen vermittelnden Standpunkt ein.

Nach der im juristischen Schrifttum überwiegend vertretenen Ansicht ist § 91 Abs. 2 AktG eng auszulegen. Er begründe keine Pflicht zur Einrichtung eines umfassenden Risikomanagementsystems.[6] § 91 Abs. 2 AktG verpflichte den Vorstand zu zwei Organisationsmaßnahmen, nämlich der Ergreifung geeigneter Maßnahmen zur Früherkennung bestandsgefährdender Entwicklungen und daneben zur Einrichtung eines unternehmensinternen Überwachungssystems, das sicherstellt, dass Innenrevision und Controlling die relevanten Erkenntnisse, insbesondere eine etwaige nachteilige Veränderung risikogeneigter Vorgänge oder Zustände, zeitnah dem Vorstand melden.[7] Demgegenüber umfasse der Risikomanagement-Prozess als Kernelemente eine Risikoidentifikation, -bewertung und -steuerung zur Entwicklung einer langfristigen und nachhaltigen Handlungsstrategie.[8] Im Vordergrund stehe dabei die Reaktion des Vorstandes auf die von dem Frühwarnsystem erkannten und übermittelten Risiken, genauer gesagt Maßnahmen der Risikobewältigung.

Für diese Auffassung wird in erster Linie der Wortlaut des § 91 Abs. 2 AktG angeführt, der die Einrichtung eines Früherkennungssystems als geeignete Maßnahme zur Sicherung des Fortbestandes der Gesellschaft bezeichnet und insoweit „insbesondere“ ein Überwachungssystem vorschreibt.

Im betriebswirtschaftlichen Schrifttum bzw. in der Prüfungspraxis wird dagegen überwiegend die Auffassung vertreten, § 91 Abs. 2 AktG stelle die Grundlage für eine Verpflichtung der Unternehmen zur Implementierung eines umfassenden Risikomanagementsystems dar.[9] Ein solches bestehe aus einem Frühwarnsystem, aus einem internen Überwachungssystem und dem Controlling. Der Begriff der Überwachung wird hier sehr streng auf die Überwachung von Risiken bezogen. Von dem Ergebnis dieser Prüfung ausgehend sei dann eine unternehmerische Entscheidung zu treffen.[10] Die interne Überwachung gewährleiste die Zuverlässigkeit der betrieblichen Prozesse, während das Controlling die Planung, Informationsversorgung, Kontrolle und Steuerung übernehme.[11] Dies umfasse auch eine Strategie zur Vermeidung, Verminderung, Überwälzung und dem Selbsttragen von Risiken.[12] Sämtliche Geschäftsvorfälle sollten dadurch auf ihr Risikopotential und ihre Gefahr für den Bestand der Gesellschaft hin untersucht werden und entsprechend behandelt werden.

6 Vgl. statt vieler: Hüffer, Aktiengesetz, 7. Auflage 2006, § 91 Rz. 9; Pahlke, NJW 2002, 1680 (1681).

7 Hüffer, Aktiengesetz, 7. Auflage 2006, § 91 Rz. 6, 8; Pahlke, Risikomanagement nach KonTraG – Überwachungspflichten für den Aufsichtsrat, NJW 2002, 1680 (1681).

8 Pampel/Krolak, in: Hauschka, Corporate Compliance, München 2007, S. 330.

9 Eggemann, Risikomanagement nach KonTraG aus dem Blickwinkel des Wirtschaftsprüfers, BB 2000, 505ff.; Lück, Elemente eines Risikomanagementsystems, DB 1998, 8.

10 Vgl. Lück, Elemente eines Risikomanagementsystems, DB 1998, 8; vgl. auch Drygala/Drygala, Wer braucht ein Frühwarnsystem, ZIP 2000, 297 (298).

11 Lück, Elemente eines Risikomanagementsystems, DB 1998, 8 (13).

12 Vgl. Eggemann, Risikomanagement nach dem KonTraG aus dem Blickwinkel des Wirtschaftsprüfers, BB 2000, 503 (506).

Diese Auffassung wird auf die Gesetzesbegründung zu § 91 Abs. 2 AktG gestützt, in der die Rede ist von einer „Verpflichtung des Vorstandes, für ein angemessenes Risikomanagement und für eine angemessene Revision zu sorgen".[13]

Die vermittelnde Auffassung greift einen Kritikpunkt an der betriebswirtschaftlichen Auffassung auf, nämlich dass sich aus § 91 Abs. 2 AktG schon deswegen keine Pflicht zur Einrichtung eines umfassenden Risikomanagementsystems ergeben könne, weil die Vorschrift nur bei existenzbedrohenden Risiken Relevanz erlange. Sie leitet aus § 91 Abs. 2 AktG einen dichteren Pflichtenstandard ab, indem primär auf den Sinn und Zweck des § 91 Abs. 2 AktG abgestellt wird, nämlich das frühzeitige Erkennen von Zuständen und Entwicklungen, die das Unternehmen bedrohen können.[14] Dieses Ziel könne nur erreicht werden, wenn die in Frage stehenden existenzbedrohenden Risiken mit Hilfe einer sinnvollen und das gesamte Unternehmen erfassenden Früherkennung bewertet, dem Vorstand anschließend mitgeteilt und die Einhaltung dieser Regeln durch eine interne Revision überwacht würden. Diese Überwachung sei in § 91 Abs. 2 AktG mit dem Begriff „Überwachungssystem" gemeint.[15]

Bei der Analyse dieser unterschiedlichen Auffassungen ist zu beachten, dass in Betriebs- und Rechtswissenschaft teilweise divergierende Definitionen für die Begriffe Risikomanagement, Risikofrüherkennung und -überwachung zugrunde gelegt werden.[16] Aber abgesehen davon hat der Streit jedenfalls im Ergebnis eine geringe praktische Bedeutung, denn wie nachfolgend noch gezeigt wird, lässt sich die Pflicht zur Einrichtung eines Risikomanagementsystems auch aus weiteren Vorschriften ableiten.

2.2 Prüfung des Frühwarnsystems durch den Abschlussprüfer

§ 317 Abs. 4 HGB bestimmt, dass bei börsennotierten Unternehmen im Rahmen der Abschlussprüfung zu beurteilen ist, ob der Vorstand die ihm nach § 91 Abs. 2 AktG obliegenden Maßnahmen in einer geeigneten Form getroffen hat und ob das interne Überwachungssystem seine Aufgaben erfüllen kann. Weitere Anhaltspunkte für die Ausgestaltung von Risikofrüherkennungssystemen liefert die Vorschrift nicht. Die rechtlichen Anforderungen an ein den Kriterien des § 91 Abs. 2 AktG genügenden Systems sind anhand betriebswirtschaftlicher Aspekte zu entwickeln.[17] Für nicht börsennotierte Aktiengesellschaften besteht die Möglichkeit, den Prüfungsauftrag

13 BT-Drucks. 13/9712, S. 15.

14 Drygala/Drygala, Wer braucht ein Frühwarnsystem, ZIP 2000, 297 (299).

15 Drygala/Drygala, Wer braucht ein Frühwarnsystem, ZIP 2000, 297 (299).

16 Bei *Seibert* ist von einem „Früherkennungssystem" die Rede, das Identifizierung, Quantifizierung, Steuerung und Kontrolle der Risiken eines Unternehmens zum Inhalt hat (Vgl. Seibert, in: Festschr. f. G. Bezzenberger (2000), 427 (437)), während diese Elemente von *Preußner/Becker* unter den Begriff des „Risikomanagementsystems" gefasst werden (Vgl. Preußner/Becker, Ausgestaltung von Risikomanagementsystemen durch die Geschäftsleitung, NZG 2002, 846 (848) Fn. 23).

17 Zimmer, in: Staub, HGB, 4. Auflage 2002, § 317 Rz. 30.

freiwillig um eine Prüfung analog § 317 Abs. 4 HGB zu erweitern, woran in erster Linie Aufsichtsräte, Konzernmuttergesellschaften und Banken ein Interesse haben.[18]

Bei den Wirtschaftsprüfern existiert für die Prüfung ein eigener Prüfstandard (PS 340).[19] Aus dem Inhalt dieses Prüfstandards lassen sich Rückschlüsse auf die Ausgestaltung des Früherkennungssystems ziehen. Auch wenn die Prüfpflicht nur für börsennotierte Unternehmen besteht, kann man dem Prüfstandard Anforderungen an ein entsprechendes System für nicht börsennotierte Aktiengesellschaften entnehmen. PS 340 stellt zunächst klar, dass zur Erkennung bestandsgefährdender Entwicklungen ein Risikofrüherkennungssystem einzurichten ist.[20] Es findet also bereits eine Konkretisierung dahingehend statt, dass es insoweit ausschließlich um Risiken für das Unternehmen geht. In dem Prüfungsbericht erfolgt keine ausführliche Darstellung des Risikofrüherkennungssystems. Nach IDW PS 340 wird die Funktionalität des Risikofrüherkennungssystems im Einzelnen auf eine Geeignetheit des Systems zu einer Identifikation der Risikofelder, zu einer Analyse und Steuerung der Risiken im Unternehmen, auf eine Fähigkeit zur Zuordnung von Verantwortlichkeiten und Aufgaben sowie zu einer Fähigkeit zur Überwachung der von den Unternehmen ergriffenen Maßnahmen überprüft. Diese Maßnahmen müssen zur Prüfung durch die Wirtschaftsprüfer angemessen dokumentiert werden.[21] Die Reaktion des Vorstandes auf erfasste und kommunizierte Risiken selbst ist nicht Gegenstand der Prüfung. Ebenso wenig gehört die Beurteilung dazu, ob die von nachgeordneten Entscheidungsträgern eingeleiteten oder durchgeführten Handlungen zur Risikobewältigung, bzw. ein Verzicht auf solche, sachgerecht oder wirtschaftlich sinnvoll ist. Mit den aufgeführten Prüfungspunkten liefert der Standard konkrete Anhaltspunkte für die Beantwortung der Frage nach der Ausgestaltung der gegenständlichen Systeme. Grundsätzlich geht es im Rahmen des § 317 Abs. 4 HGB nicht darum, ob der Vorstand auf ein erkanntes Risiko angemessen und erfolgreich reagiert hat und geeignete Risikobewältigungsmaßnahmen ergriffen hat.[22] In der Prüfungspraxis hingegen richtet der Abschlussprüfer sein Augenmerk sehr wohl auf die Reaktionen des Vorstandes und die von ihm ergriffenen Maßnahmen. Im Rahmen der Systemprüfung unter dem Prüfungspunkt der Zuordnung von Verantwortlichkeiten und Aufgaben und der Überwachung der Effektivität und Angemessenheit werden nämlich für den Abschlussprüfer bei einer risikoorientierten Prüfung insbesondere Maßnahmen zur Risikosteuerung und -überwachung von Interesse sein. Insoweit verschwimmt die Trennlinie zwischen Früherkennungssystem und Risikomanagementsystem, eine Differenzierung wird insoweit nicht immer vorgenommen und ist in praxi auch nicht möglich.[23]

18 Vgl. Eggemann, Risikomanagement nach dem KonTraG aus dem Blickwinkel des Wirtschaftsprüfers, BB 2000, 503 (506).

19 Abgedruckt in WpG 1999, S. 658ff.

20 Vgl. WpG 1999, S. 658.

21 WpG 1999, S. 658.

22 Vgl. WpG 1999, S. 658.

23 Vgl. Wiedmann, in: IDW, WP Handbuch, 13. Auflage 2006, S. 2115.

2.3 Inhalt des Lageberichts

Dass es mit der Früherkennung von Risiken durch ein entsprechendes Überwachungssystem nicht getan sein kann, folgt bereits aus den ebenfalls mit dem KonTraG eingeführten ergänzenden Vorschriften zur Rechnungslegung. § 289 Abs. 1 Satz 4 HGB verlangt eine Beurteilung und Erläuterung der voraussichtlichen Entwicklung mit ihren wesentlichen Chancen und Risiken. Noch detaillierter verlangt § 289 Abs. 2 Ziffer 2 HGB im Lagebericht die folgenden Angaben:

„a) Die Risikomanagementziele und -methoden der Gesellschaft einschließlich ihrer Methoden zur Absicherung aller wichtiger Arten von Transaktionen, die im Rahmen der Bilanzierung von Sicherungsgeschäften erfasst werden, sowie
b) die Preisänderungs-, Ausfall- und Liquiditätsrisiken sowie die Risiken aus Zahlungsstromschwankungen, denen die Gesellschaft ausgesetzt ist,

jeweils in Bezug auf die Verwendung von Finanzinstrumenten durch die Gesellschaft und sofern dies für die Beurteilung der Lage oder der voraussichtlichen Entwicklung von Belang ist."

Wie sich aus dem letzten Halbsatz dieser Vorschrift ergibt, will man damit in erster Linie Finanzinstrumente erfassen, insbesondere Hedge-Geschäfte in Form von Derivaten. Zumindest in diesem Bereich verlangt das Gesetz nicht nur eine Darstellung der Risiken, sondern eben auch Risikomanagementziele und -methoden. Zusammen mit der Verpflichtung zur Früherkennung von Risiken wird man daraus zumindest für den Bereich der durch Hedge-Geschäfte absicherbaren Transaktionen ein vollständiges Risikomanagementsystem ableiten können. Denn sonst könnte es im Lagebericht nicht dargestellt werden. Dabei mögen Schieflage in Unternehmen aus dem spekulativen Einsatz von Derivaten (Beispiele gab es bei der Metallgesellschaft, der DG-Bank und Volkswagen) dazu beigetragen haben, hier gesetzgeberisch einen Schwerpunkt im Risikomanagement zu setzen.

Zukünftig dürfte allerdings aus europarechtlichen Gründen die Darstellung im Lagebericht deutlich ausführlicher ausfallen und sich auch auf ein allgemeines Risikomanagementsystem erstrecken. Nach dem Aktionsplan der EU-Kommission vom 21.05.2003 „Modernisierung des Gesellschaftsrechts und Verbesserung der Corporate Governance in der Europäischen Union"[24], in dem ein Schwerpunkt auf eine Reihe von Initiativen zur Corporate Governance gesetzt wurde, ist am 05.09.2006 die Richtlinie zur Abänderung der 4. und 7. EG-Richtlinie (Abänderungs-Richtlinie)[25] in Kraft getreten. Diese ist bis zum 05.09.2008 in nationales Recht umzusetzen (Art. 5 Abänderungs-Richtlinie). Die relevanten Änderungen ergeben sich bei der 4. und 7. EU-Richtlinie vor allem durch die Einführung von Art. 46a. Dieser fordert von Unternehmen, deren Wertpapiere zum Handel am geregelten Markt im Sinne der Europäischen Union zugelassen sind, eine Beschreibung der wichtigsten Merkmale des internen Kontroll- und Risikomanagementsystems der Gesellschaft im Hinblick auf den Rechnungslegungsprozess.[26] Diese Beschreibung ist Teil eines jährlich zu

24 Vgl. IP/03/716 und MEMO/03/112, abrufbar unter: http://europa.eu.
25 RL 2006/46/EG, Abl. L 224 vom 16.08.2006, S. 1–7.
26 Art. 46a Abs. 1 lit. c) der 4. EG-Richtlinie.

veröffentlichenden „Corporate Governance Statements". Im Gegensatz zu der von der Hochrangigen Expertengruppe[27] und der Kommission[28] vorgeschlagenen Fassung schreibt die nunmehr endgültige Fassung der Richtlinie keine Beschreibung des gesamten, sondern lediglich des rechnungslegungsbezogenen Teils des internen Kontroll- und Risikomanagements vor.

Theoretisch ist sowohl nach der Richtlinie, als auch nach dem HGB im Bezug auf Absicherungsgeschäfte vorstellbar, dass der Lagebericht an dieser Stelle eine Negativerklärung enthält, dass Risikomanagementsysteme nicht vorhanden sind. Art. 46a ist jedoch keinesfalls so zu verstehen, dass die betreffenden Unternehmen zur Einrichtung von internen Kontroll- und Risikomanagementsystemen nur im Hinblick auf den Rechnungslegungsprozess verpflichtet sind. Die Beschränkung nach dieser Vorschrift bezieht sich ausweislich ihres Wortlautes ausschließlich auf die Beschreibung innerhalb des „Corporate Governance Statements". Hinter den genannten Vorschriften verbirgt sich indes vielmehr die Annahme, dass eine Gesellschaft üblicherweise über solche Instrumentarien verfügen muss. Sie sind daher Indikatoren dafür, dass die Rechtsordnung allgemein von der Existenz von Risikomanagementsystemen als Teil einer „best practice" ausgeht.

3. Allgemeine Geschäftsleitungspflicht

Aus § 76 Abs. 1 AktG ergibt sich die allgemeine Leitungspflicht des Vorstands, § 93 Abs. 1 Satz 1 AktG konkretisiert den dabei anzulegenden Sorgfaltsmaßstab. Hinsichtlich einer Risikomanagementpflicht des Vorstands ist die Verpflichtung der Vorstandsmitglieder bedeutsam, den Unternehmenserfolg im Rahmen des Gesetzes, der Satzung und der verbindlichen Beschlüsse von Aufsichtsrat und Hauptversammlung unter Berücksichtigung des Unternehmensinteresses zu fördern und Schäden für die Gesellschaft zu verhindern.[29] Selbst wenn man § 91 Abs. 2 AktG so verstanden wissen will, dass sich daraus direkt keine Verpflichtung zur Einrichtung von Risikomanagementsystemen zur Risikohandhabung ergibt, verlangt § 76 Abs. 1 AktG und der anzulegende Sorgfaltsmaßstab den angemessenen Umgang des Vorstands mit Risiken. Daraus ergibt sich bereits, dass das Risikomanagement eine originäre Leitungspflicht des Vorstands darstellt.

Gemäß § 90 Abs. 1 AktG hat der Vorstand diverse Berichtspflichten gegenüber dem Aufsichtsrat, die die künftige Geschäftspolitik und Unternehmensplanung betreffen. Damit korrespondieren entsprechende Informationsrechte des letzteren. Daraus ergibt sich, dass sich der Vorstand stets ein genaues Bild von der Lage des Unternehmens verschaffen muss und die grundsätzlichen Entscheidungen bezüglich der Unternehmensplanung zu treffen hat. Diese Entscheidungen erfordern neben der sorgfältigen Beurteilung bereits bestehender oder sich künftig entwickelnder Risiken auch einen pflichtgemäßen Umgang mit bekannt gewordenen Risiken.[30] Be-

27 Vgl. Bericht der Hochrangigen Expertengruppe über Moderne Gesellschaftsrechtliche Rahmenbedingungen in Europa, 2002, S. 49.

28 Vgl. Art. 46a Abs. 1 Nr. 3 der 4. EG-Richtlinie.

29 Vgl. etwa Hüffer, Aktiengesetz, 7. Auflage 2006, § 93 Rn. 3.

30 Wiesner, Münchener Handbuch des Gesellschaftsrechts, 3. Auflage 2007, Bd. IV, § 25 Rn. 7.

standsgefährdende Risiken müssen auch dann erkannt werden, wenn mit ihrer tatsächlichen Realisierung erst langfristig zu rechnen ist.

Die Beantwortung der Frage, ob ein Geschäftsleiter bei der Erfüllung seiner Leitungspflicht ordnungsgemäß und gewissenhaft gehandelt hat, bemisst sich unter anderem danach, welches Handeln von ihm einerseits das Gesetz, andererseits die betroffenen Verkehrskreise erwarten und wie die tatsächliche Übung im sonstigen Geschäftsverkehr ist. Vergleichsgröße sind Leiter anderer Unternehmen ähnlicher Art und Größe, die nicht mit eigenen Mitteln wirtschaften, sondern treuhänderisch fremde Vermögen verwalten.[31] Zwar stellt die Eingehung von Risiken eine dem Vorstand obliegende Ermessensentscheidung dar.[32] Daher ist die Frage nach einer möglichen Pflichtverletzung insoweit durchaus sensibel, da sie den Kernbereich individuellen unternehmerischen Handelns betrifft und aus der ex-post-Perspektive oft schwierig zu beantworten ist. Es ist jedoch unerlässlich, von einem besonnenen und dem Unternehmensinteresse verhafteten Geschäftsleiter zu fordern, ein System einzurichten, das rechtzeitig bestehende Risiken erkennt. Das Abwarten des Risikoeintritts wird für die Vorbereitung geeigneter Maßnahmen zur Risikoabwehr in der Regel zu spät sein. Damit obliegt dem Vorstand aufgrund seiner allgemeinen Leitungspflicht sogar eine über das von § 91 Abs. 2 AktG geforderte Maß hinausgehende Verpflichtung zur Risikoerkennung und präventiven Risikobewältigung.

4. Deutscher Corporate Governance Kodex

Auch der deutsche Corporate Governance Kodex (DCGK) beschäftigt sich mit dem Risikomanagement als Leitungsaufgabe in börsennotierten Aktiengesellschaften. Er enthält eine Reihe von Regelungen, die sich mit dem Risikomanagement befassen.

4.1 Zielsetzung und Wirkungsweise des DCGK

Der DCGK zielt darauf ab, „das deutsche Corporate Governance System transparent und nachvollziehbar zu machen und das Vertrauen der Anleger, der Kunden, der Mitarbeiter und der Öffentlichkeit in die Leitung und Überwachung deutscher börsennotierter Aktiengesellschaften [zu] fördern". Die Regierungskommission Deutscher Corporate Governance Kodex hat jüngst Änderungen des Kodex' beschlossen, die Neufassung wurde am 20. Juli 2007 durch das Bundesministerium der Justiz im elektronischen Bundesanzeiger bekannt gemacht.[33]

Ausweislich seiner Präambel enthält der DCGK eine Darstellung wesentlicher gesetzlicher Vorschriften zur Leitung und Überwachung deutscher börsennotierter Gesellschaften sowie international und national anerkannter Standards guter und verantwortungsvoller Unternehmensführung. Der Kodex nimmt also für sich in Anspruch, über weite Passagen den Zustand des deutschen Rechts der Unternehmens-

31 BGHZ 129, 30 (34) = NJW 1995, 1290.

32 BGHZ 125, 239 (246); 135, 245 (253).

33 Bundesministerium der Justiz, Bekanntmachung des „Deutschen Corporate Governance Kodex" in der Fassung vom 14. Juni 2007, Bundesministerium der Justiz (Hrsg.), Elektronischer Bundesanzeiger vom 20. Juli 2007, Präambel.

führung darzustellen. Nur wenn der Kodex das Wort „soll" verwendet, handelt es sich um eine über die rechtlichen Anforderungen hinausgehende Empfehlung und soweit der Kodex die Worte „sollte" oder „kann" benutzt, handelt es sich um so genannte Anregungen. Für nicht börsennotierte Unternehmen gilt der DCGK nicht, wenngleich auch diesen die Beachtung empfohlen wird.

Es steht deutschen börsennotierten Unternehmen frei, ob sie den Empfehlungen oder Anregungen des Kodex folgen wollen. Nach § 161 AktG sind der Vorstand und der Aufsichtsrat einer börsennotierten Gesellschaft allerdings verpflichtet, jährlich zu erklären, dass dem DCGK entsprochen wurde oder welchen Empfehlungen nicht gefolgt wurde oder wird. Abweichungen von Anregungen des DCGK müssen nicht offen gelegt werden. Die Standards des DCGK können als Vergleichskriterien bei der Beantwortung der Frage dienen, ob einzelne Risikomanagementmaßnahmen den gesetzlichen Anforderungen an die Unternehmensführung genügen.[34] Der DCGK enthält unter dem Stichwort des Risikomanagements Regelungen über die Organisation, Aufgabe, Funktion und Zusammenarbeit der internen und externen Überwachungsträger in deutschen Kapitalgesellschaften.[35]

4.2 Vorschriften zum Risikomanagement

Ziffer 5.2 Abs. 3 DCGK enthält die Empfehlung, dass der Aufsichtsratsvorsitzende mit dem Vorstand regelmäßig Kontakt halten und mit ihm das Risikomanagement des Unternehmens beraten soll.

Ziffer 5.3.2 DCGK empfiehlt, dass der Aufsichtsrat einen Prüfungsausschuss (Audit Committee) einrichten soll, der sich insbesondere mit Fragen des Risikomanagements befasst.

Dagegen sind die Vorstandspflichten zum Risikomanagement nicht als Empfehlungen formuliert, sondern als Darstellung des geltenden Rechtszustandes. In Ziffer 4.1.4 DCGK heißt es lapidar:

„Der Vorstand sorgt für ein angemessenes Risikomanagement und Risikocontrolling im Unternehmen."

Ziffer 3.4 Abs. 2 DCGK lautet:

„Der Vorstand informiert den Aufsichtsrat regelmäßig, zeitnah und umfassend über alle für das Unternehmen relevanten Fragen . . . der Risikolage und des Risikomanagements."

Zentrale Punkte der Corporate Governance in einem börsennotierten Unternehmen sind einerseits seine Leitung durch den Vorstand, andererseits die Überwachung des Vorstandes durch den Aufsichtsrat. Der Begriff der Überwachung wird dabei weiter gefasst als in § 91 Abs. 2 AktG. Er sieht eine Unternehmensüberwachung vor, die neben der Risikofrüherkennung auch organisatorische Kontroll- und Sicherungsmaßnahmen sowie eine interne Revision umfasst. Die Verfasser des DCGK sind somit zu der Schlussfolgerung gelangt, dass wohl jedes börsennotierte Unternehmen von Rechts wegen über ein Risikomanagement und Risikocontrolling verfügen muss. Faktisch stellt der DCGK über die Entsprechens-Erklärung in § 161

34 vgl. v. Randow, Derivate und Corporate Governance, ZGR 1996, 594 (625).

35 Punkte 3.4; 4.1.3; 5.2; 5.3.2 des DCGK.

AktG zumindest eine indirekte Verpflichtung für die Unternehmensleitung dar, da sie sich für nicht befolgte Empfehlungen regelmäßig gegenüber Aktionären, Banken, anderen Gläubigern, Investoren und sonstigen Geschäftspartnern rechtfertigen muss. Diese erwarten in der Regel, dass „best practice"-Verhaltensregeln befolgt werden. Es wird insoweit vielfach von einer mittelbaren Pflicht der börsennotierten Aktiengesellschaften zur Befolgung gesprochen.[36]

5. Die neue Baseler Eigenkapitalvereinbarung (Basel II)[37]

Mit den als „Basel II" bekannt gewordenen Vorschriften zur Eigenkapitalunterlegung in Banken sind mittelbar ebenfalls Normen gesetzt worden, die auch das Risikomanagement von Unternehmen allgemein betreffen.

Die Basel II-Vorschriften wurden vom Baseler Ausschuss für Bankenaufsicht vorgeschlagen und nach dem so genannten „Eigenmittelakkord" in Europäisches Gemeinschaftsrecht und nationales Recht umgesetzt. Die Inkorporierung von Basel II in das Europäische Gemeinschaftsrecht erfolgte durch die Neufassung der EU-Richtlinien 2006/48/EG[38] („Bankenrichtlinie") und 2006/49/EG[39] („Kapitaladäquanzrichtlinie"). In Deutschland erfolgte die Umsetzung durch das „Gesetz zur Umsetzung der neu gefassten Bankenrichtlinie und der neu gefassten Kapitaladäquanzrichtlinie" vom 17.11.2006, das zum 01.01.2007 in Kraft trat.

Die Basel II-Vereinbarung besteht aus drei sich gegenseitig verstärkenden Säulen, die zusammen zu einem sicheren und soliden Finanzsystem beitragen sollen. Die Umsetzung der Richtlinien wurde für die zweite Säule durch Änderungen im Kreditwesengesetz (7. KWG-Novelle) erreicht, das insoweit durch die „Mindestanforderungen an das Risikomanagement" (MaRisk) konkretisiert wird, sowie für die erste und dritte Säule durch die Solvabilitätsverordnung (SolvV).

Säule 1[40] beinhaltet Vorschriften zur Eigenmittelunterlegung von Kreditausfall-, Marktpreis- und operationellen Risiken. Säule 2[41] gibt eine laufende und regelmäßige Überprüfung der Banken durch die Bankenaufsicht vor. Die Aufsicht hat sicherzustellen, dass jede Bank über das entsprechende interne Risikomanagementverfahren verfügt und dieses auch funktioniert. Säule 3[42] (Marktdisziplin) zielt darauf ab, Kreditinstituten umfassendere Publizitätspflichten aufzuerlegen, um einen besseren Einblick in das Risikoprofil einer Bank und die Angemessenheit der Eigenkapitalausstattung zu ermöglichen und durch Verbesserung der Transparenz eine Stärkung der Marktdisziplin zu erzielen.

36 Ulmer, Der Deutsche Corporate Governance Kodex – ein neues Regulierungsinstrument für börsennotierte Aktiengesellschaften, ZHR 166 (2002), 150.

37 Abrufbar unter http://www.bis.org.

38 Bislang: Richtlinie 2000/12/EG des Europäischen Parlaments und des Rates vom 20.3.2000 über die Aufnahme und Ausübung der Tätigkeit der Kreditinstitute.

39 Bislang: Richtlinie 93/6/EWG des Rates vom 15.3.1993 über die angemessene Eigenkapitalausstattung von Wertpapierfirmen und Kreditinstituten.

40 Vgl. Teil 2: Säule 1 – Mindestkapitalanforderungen.

41 Vgl. Teil 3: Säule 2 – Aufsichtsrechtliches Überprüfungsverfahren.

42 Vgl. Teil 4: Säule 3: Marktdisziplin.

Nach den Vorgaben von Basel II sind Banken verpflichtet, bei der Kreditvergabe ein Rating ihrer Kunden vorzunehmen. Dieser Ratingprozess beinhaltet die Überprüfung sämtlicher Faktoren, also der Stärken und Schwächen der jeweiligen Unternehmens. Ein nicht unwesentlicher Teil des Kreditratings wird auch davon abhängen, welche Risikomanagementmaßnahmen im Unternehmen getroffen wurden. Nur wenn die Kreditinstitute ihr eigenes Risiko bei der Gewährung von Krediten minimieren können, werden sie liquide Mittel zur Verfügung stellen. Von den Unternehmen in ihrer Eigenschaft als Kreditnehmer wird auf diese Weise indirekt gefordert, die Voraussetzung für eine positive Beurteilung im Ratingverfahren der Banken zu schaffen. Die Anforderungen der Banken oder Ratingagenturen bei der Festlegung des Ratings werden zukünftig einen weiteren Standard für ein Risikomanagementsystem setzen, da es als unternehmensinterner Prozess die Grundlage für eine unternehmerische Risikodarstellung und -transparenz bildet sowie eine wertorientierte Steuerung des Unternehmens. Die allgemeinen Pflichten des Vorstands werden es deshalb zukünftig gebieten, zur Rating-Verbesserung Risikomanagementsysteme einzuführen oder bestehende Systeme zu optimieren. Dies gilt umso mehr, als in Zeiten harten Wettbewerbs auf den Märkten die Eingehung von Risiken aus unternehmerischer Sicht unumgänglich ist und Risiken stets auch als Chancen begriffen werden.

6. Bankaufsichtsrecht

Der Geschäftsbetrieb von Kreditinstituten und Finanzdienstleistern ist streng reguliert, insbesondere durch das Kreditwesengesetz (KWG) und das Wertpapierhandelsgesetz (WpHG). Ein zentrales Instrument sind bankaufsichtsrechtlich definierte Organisationspflichten. § 25a KWG verlangt in Abs. 1 Satz 1, dass ein Institut über eine ordnungsgemäße Geschäftsorganisation verfügen muss, die die Einhaltung der von den Instituten zu beachtenden gesetzlichen Bestimmungen gewährleistet. § 25a Abs. 1 Satz 3 Ziffer 1 KWG bestimmt in seiner durch Gesetz vom 17.11.2006[43] geänderten Form, dass eine ordnungsgemäße Geschäftsorganisation insbesondere umfasst:

„ein angemessenes Risikomanagementsystem. Dies beinhaltet auf der Grundlage von Verfahren zur Ermittlung und Sicherstellung der Risikotragfähigkeit die Festlegung von Strategien sowie die Einrichtung interner Kontrollverfahren, die aus einem internen Kontrollsystem und einer internen Revision bestehen, wobei das interne Kontrollsystem dabei insbesondere umfasst:

a) aufbau- und ablauforganisatorische Regelungen, die eine klare Abgrenzung der Verantwortungsbereiche umfassen, und
b) Prozesse zur Identifizierung, Beurteilung, Steuerung sowie Überwachung und Kommunikation der Risiken; dabei soll den im Anhang V der Bankenrichtlinie niedergelegten Kriterien Rechnung getragen werden."[44]

43 BGBl. I S. 2606.

44 Der Hinweis auf Anhang V der Bankenrichtlinie dient der Konkretisierung der insoweit zu betrachtenden Risikobereiche und den hierbei anzuwendenden Kriterien, vgl. Basel II-Gesetz, Begründung zu Art. 1 Nr. 33 a) aa) (S. 62).

Infolge dieser Gesetzesänderung verwendet der Gesetzgeber nunmehr erstmals explizit den Begriff des Risikomanagements und erläutert ihn, nachdem § 25a Abs. 1 Satz 1 KWG a. F. lediglich

„... geeignete Regelungen zur Steuerung, Überwachung und Kontrolle der Risiken und der Einhaltung der gesetzlichen Bestimmungen sowie (...) angemessene Regelungen (...) anhand deren sich die finanzielle Lage des Instituts oder der Gruppe jederzeit mit hinreichender Wahrscheinlichkeit bestimmen lässt" (Ziff. 1)

bzw. in Ziffer 2

„... eine ordnungsgemäße Geschäftsorganisation, über ein angemessenes internes Kontrollverfahren sowie über angemessene Sicherheitsvorkehrungen für den Einsatz der elektronischen Datenverarbeitung" (Ziff. 2) vorschrieb.

Auch wenn § 25a KWG nur einen Rahmen für die Definition eines angemessenen Risikomanagements liefert und die Vorschrift direkt nur einen begrenzten Adressatenkreis betrifft, bietet sie doch auch Interpretationshilfen im Hinblick auf die Pflichten von Unternehmen, die nicht unmittelbar angesprochen sind.

Zur näheren Konkretisierung hat die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) als zuständige Behörde vor Kurzem zusammengefasste „Mindestanforderungen an das Risikomanagement – MaRisk" erlassen.[45] Die MaRisk fassen die bisherigen Mindestanforderungen zum Kreditgeschäft (MaK) und zum Handelsbuchgeschäft (MaH) zusammen, straffen und flexibilisieren sie und formulieren zum allgemeinen Risikomanagement auch neue Verpflichtungen.

Die MaRisk sind modular aufgebaut und befassen sich im allgemeinen Teil eingehend mit den Risikoarten, der Einrichtung eines internen Kontrollsystems und der Einführung angemessener Risikosteuerungs- und Controllingprozesse, die eine Identifizierung, Beurteilung, Steuerung sowie Überwachung und Kommunikation der wesentlichen Risiken gewährleisten sollen, wobei diese Prozesse in ein integriertes System zur Ertrags- und Risikosteuerung („Gesamtbanksteuerung") eingebunden werden sollen (Ziffer AT 4.3.2 MaRisk). Hierbei müssen die Risikosteuerungs- und Controllingprozesse gewährleisten, dass die wesentlichen Risiken frühzeitig erkannt, vollständig erfasst und in angemessener Weise dargestellt werden können. Weiter müssen für die zu berücksichtigenden Risiken angemessene Szenariobeobachtungen angestellt werden. Die Geschäftsleitung hat sich in angemessenen Abständen über die Risikosituation und die Ergebnisse der Szenariobeobachtungen berichten zu lassen, wobei in die Risikoberichterstattung bei Bedarf auch Handlungsvorschläge zur Risikoreduzierung aufzunehmen sind. Die MaRisk zielen insbesondere auf die Einrichtung angemessener institutsinterner Leitungs-, Steuerungs- und Kontrollprozesse ab und betonen die Bedeutung des Aufsichtsorgans für die Wahrnehmung der Überwachungsfunktion (AT 1 Tz. 1).

Ziffer AT 5 der MaRisk bestimmt weiter, dass die entsprechenden Regelungen, einschließlich der Regelung zur internen Revision, in Organisationsrichtlinien schriftlich festzuhalten und den betroffenen Mitarbeitern in geeigneter Weise bekannt gemacht werden müssen.

45 Abrufbar auf der Webseite der BaFin unter www.bafin.de, Rechtliche Grundlagen – Verlautbarungen und Rundschreiben – Rundschreiben 2005 in der Fassung vom 06.03.2007.

Es stellt sich die Frage, welche Ausstrahlungswirkungen § 25a KWG und die MaRisk auf die Anforderungen an das Vorhandensein und die Ausgestaltung eines Risikomanagementsystems außerhalb des Bereichs der Banken und Finanzdienstleister haben. Der allgemeine Teil der MaRisk ist weitgehend auch auf Unternehmen anderer Branchen übertragbar, denn es geht darin um grundlegende Anforderungen und insbesondere die Prinzipien für die Ausgestaltung des Risikomanagementsystems. Der allgemeine Teil nimmt keinen unmittelbaren Bezug auf bestimmte Geschäftsarten oder Risiko-Kategorien. In diesem Zusammenhang werden Anforderungen hinsichtlich Risiko-Tragfähigkeit, Strategie, internes Kontrollsystem und interne Revision geregelt. In einem besonderen Teil werden die spezifischen Anforderungen an die Aufbau- und Ablauforganisation im Kredit- und Handelsgeschäft, die Prozesse zur Identifizierung, Beurteilung, Steuerung, Überwachung und Kommunikation bestimmter Risiken sowie die interne Revision beschrieben. Neben verschiedenen Äußerungen in der Literatur[46] zu diesem Thema haben sich in jüngerer Zeit auch zwei Gerichte für eine solche Ausstrahlungswirkung ausgesprochen.

In einer Entscheidung des Verwaltungsgerichts Frankfurt am Main[47] wurde für ein Versicherungsunternehmen über die Vorschrift des § 91 Abs. 2 AktG der § 25a Abs. 1 KWG a. F. zur Auslegung herangezogen. Das Gericht führt aus, dass der Gesetzgeber bei der Einführung des § 91 Abs. 2 AktG bereits davon ausging, dass der Vorstand einer Aktiengesellschaft als Teil seiner Leitungsaufgabe für ein angemessenes Risikomanagement zu sorgen hat. Weiter führt das Gericht aus, dass sich § 91 Abs. 2 AktG und § 25a Abs. 1 KWG in ihrer rechtlichen Bedeutung entsprechen, so dass die in § 25a Abs. 2 KWG gesetzlich genauer gefassten Anforderungen bei der Auslegung des § 91 Abs. 2 AktG herangezogen werden können.[48]

In ähnlicher Weise hat sich das Landgericht Berlin für den Fall der Kündigung eines Vorstandsmitglieds einer Hypothekenbank aus wichtigem Grund geäußert. Dem Vorstand war im Rahmen der fristlosen Kündigung seines Dienstverhältnisses vorgeworfen worden, die von ihm getroffenen Maßnahmen zum Risikomanagement erfüllten nicht die gesetzlichen Anforderungen. Das Gericht geht in seiner Entscheidung[49] von einer Pflichtenidentität von § 25a KWG und § 91 Abs. 2 AktG aus.

Wenn man – wie die beiden Gerichte – von einer Pflichtenidentität ausgeht, verblieben für einen Vorstand dennoch Unklarheiten, da § 25a Abs. 1 KWG – konkretisiert durch die MaRisk – lediglich Mindestanforderungen formuliert. Wie weit die Organisationspflichten im Einzelnen gehen ist branchen- und unternehmensabhängig und steht im Leitungsermessen des Vorstandes. In diesem Sinne ist auch die Frage einer rechtlich verpflichtenden Ausstrahlungswirkung des § 25a Abs. 1 KWG zu beantworten. Den Kritikern, die dieser Interpretation mit dem Argument entgegentre-

46 Vor allem Preußner/Zimmermann, Risikomanagement als Gesamtaufgabe des Vorstands, AG 2002, S. 657ff., insb. S. 659f.; Preußner, Risikomanagement im Schnittpunkt von Bankaufsichtsrecht und Gesellschaftsrecht, NZG 2004, S. 57ff., insb. 59f., Fleischer, Zur Leitungsaufgabe des Vorstands im Aktienrecht, ZIP 2003, S. 1ff.

47 VG Frankfurt, Urteil vom 08.07.2004 – 1 E 7363/03, AG 2005, S. 264.

48 VG Frankfurt, Urteil vom 08.07.2004 – 1 E 7363/03, AG 2005, S. 265.

49 LG Berlin, Urteil vom 03.07.2002 – 2 O 358/01, AG 2002, 682ff, kommentiert von Preußner/Zimmermann, Risikomanagement als Gesamtaufgabe des Vorstands, AG 2002, S. 657ff.

ten, auf diese Weise wäre § 91 Abs. 2 AktG aufgrund des Spezialnorm-Charakters des § 25a Abs. 1 KWG überflüssig[50], ist der Wortlaut des § 91 Abs. 2 AktG entgegenzuhalten, der von „geeigneten Maßnahmen" spricht und ein Überwachungssystem als „insbesondere"-Maßnahme erwähnt. Zwar ist allgemein anerkannt, dass Spezialnormen allgemeine Vorschriften grundsätzlich lediglich innerhalb ihres Anwendungsbereichs konkretisieren. Indem § 25a KWG und die MaRisk grundlegende Anforderungen an den Umgang mit Risiken aufstellt, eignen sie sich auch zu der in dieser Hinsicht vorzunehmenden Beurteilung der Rechtmäßigkeit von Organhandlungen von Nicht-Kreditinstituten. Dies gilt insbesondere z. B. im Zusammenhang mit Investitions- oder Kreditgeschäften. Insoweit ist die MaRisk geradezu prädestiniert, um für die Auslegung des § 91 Abs. 2 AktG herangezogen zu werden. Es besteht insofern ein Zusammenhang zwischen den Regelungsbereichen, so dass die Heranziehung der Spezialvorschrift zur Auslegung des § 91 Abs. 2 AktG in gesetzessystematischer Hinsicht nicht zu beanstanden ist[51] – ausgehend von der Annahme, dass die konkrete Ausgestaltung des Risikomanagementsystems auf einer Ermessensentscheidung des Geschäftsleiters basiert und unter anderem von der Größe und Struktur des betreffenden Unternehmens und der jeweiligen Branche abhängt.

Auch wenn es damit noch nicht „Mainstream" ist, von einer Pflichtenidentität und damit von einer Ausstrahlungswirkung des § 25a KWG auf andere Branchen auszugehen, definiert das Bankaufsichtsrecht, insbesondere auch die MaRisk, einen „best practice" Standard, an dem sich umsichtige Unternehmensleiter orientieren sollten.

7. Sarbanes-Oxley Act[52]

Zu einem solchen „best practice" Standard können auch Verpflichtungen nach dem US-amerikanischen Sarbanes-Oxley Act von 2002 beitragen, der infolge der amerikanischen Bilanzskandale von Enron oder Worldcom erlassen wurde. Unmittelbar betrifft er zwar lediglich die an der US-amerikanischen Wertpapierbörse zugelassenen deutschen Unternehmen. Des Weiteren müssen auch deutsche Tochterunternehmen US-amerikanischer börsennotierter Unternehmen ihre Berichterstattung an die Vorgaben des Sarbanes-Oxley Acts anpassen. Damit kommt ihm auch eine exterritoriale Wirkung zu.

Nach Sec. 404 des Sarbanes-Oxley Act (Management Assessment of International Controls) ist als Teil der Geschäftsberichte ein „Internal Control Report" zu erstellen, der von dem Abschlussprüfer geprüft und bestätigt wird.[53] Dabei handelt es sich um ein Risikokontrollsystem, in dem durch Ausführungen zu den Unternehmensprozessen eine Kontrolle der Zahlen für die Finanzberichterstattung stattfindet, um auf diese Weise das Risiko fehlerhafter Bilanzen zu minimieren. Die Bestätigung

50 Bürkle, Auswirkungen der Unternehmensaufsicht nach dem KWG auf organisatorische Pflichten von Versicherungsnehmen, WM 2005, 1496 (1499).

51 A. A. Bürkle, Auswirkungen der Unternehmensaufsicht nach dem KWG auf organisatorische Pflichten von Versicherungsunternehmen, WM 2005, 1496 (1498).

52 Abrufbar unter http://www.law.uc.edu.

53 Sec. 404 b Sarbanes-Oxley Act.

durch den Wirtschaftsprüfer ist Teil des Prüfungsauftrages zur Prüfung des Jahresabschlusses. Da es sich dabei nicht um einen unabhängigen Auftrag handelt, kann sich der Abschlussprüfer nicht durch eine Separierung der Aufträge der Bestätigung entziehen. Im Unterschied zur Prüfung der Risikofrüherkennungssysteme in § 317 Abs. 4 HGB wird im US-amerikanischen Recht eine allgemeine Zusicherung zur Funktionsfähigkeit des internen Kontrollsystems erwartet, es sollen nicht nur bestandsgefährdende Risiken abgewendet werden.[54] Die Verpflichtungen nach dem Sarbanes-Oxley Act gehen damit in nicht unerheblicher Weise über die deutschen Anforderungen hinaus. Es ist zu erwarten, dass die Unternehmen die Anforderungen des Sarbanes-Oxley Acts als Elemente guter Corporate Governance anerkennen und sie in Folge dessen auch von Unternehmen beachtet werden, die dazu nicht direkt verpflichtet sind.[55]

8. Compliance

Es bedarf eigentlich keiner Erwähnung, dass Unternehmen und ihre Organe sich bei ihrem Handeln an das geltende Recht zu halten haben. Dass dies jedoch in der Praxis nicht selbstverständlich ist, zeigt sich anhand verschiedener in jüngerer Vergangenheit bekannt gewordener Fälle der Wirtschaftskriminalität in deutschen Unternehmen, anhand von Kartellverstößen, die durch Rekordbußgelder sanktioniert wurden oder diversen Unternehmenskrisen, zu denen es durch Gesetzesverstöße gekommen ist, an denen teilweise die Unternehmensleitungen in erheblicher Weise beteiligt waren.

Im Zusammenhang mit Risikomanagementsystemen ist deshalb auch der Begriff der „Compliance" zu nennen. Nach den jüngsten Änderungen des Corporate Governance Kodex wurde dieses Schlagwort aufgegriffen und in dem Kodex in Ziffer 4.1.3 wie folgt definiert:

„Der Vorstand hat für die Einhaltung der gesetzlichen Bestimmungen und der unternehmensinternen Richtlinien zu sorgen und wirkt auf deren Beachtung durch die Konzernunternehmen hin (Compliance)."

Compliance-Programme haben in der Praxis eine Präventivfunktion. Durch sie sollen problematische Sachverhalte und Strukturen vermieden, frühzeitig aufgedeckt und potentielle Verstöße möglichst schon im Vorfeld erkannt werden. Wirtschaftkriminelle Handlungen müssen in die Gefährdungsanalyse mit einbezogen werden. Compliance-Systeme sollten so ausgestaltet sein, dass sie einen umfassenden Schutz für das Unternehmen darstellen. Regelverstöße von Mitarbeitern werden insoweit als wirtschaftliches Risiko für die Unternehmen und zunehmend auch für die Unternehmensleitung verstanden. Es geht dabei nicht darum, Mitarbeiter auf gesetzestreues Handeln hin zu überwachen. Dieses sollte selbstverständlich sein. Das Unternehmen muss vielmehr Schwerpunkte setzen, welche gesetzlichen Anforderungen für die Unternehmenstätigkeit von hoher Relevanz und besonders risikorelevant sind. Wenn die diesbezüglich wesentlich betroffenen Mitarbeiter identifi-

54 Lanfermann/Maul, Auswirkungen des Sarbanes-Oxley Acts in Deutschland, Der Betrieb 2002, 1725 (1727).

55 So auch Ringleb, Deutscher Corporate Governance Kodex, München 2005.

ziert sind, stellt sich für die Geschäftleitung die Frage, wie durch organisatorische Maßnahmen eine Compliance im Unternehmen sichergestellt werden kann.

Gesteigerte Unternehmensrisiken drohen z. B. im Bereich des Kartellrechts, des Umwelt- oder Kapitalmarktrechts. Die Intensivierung der Verfolgungstätigkeit der Kartellbehörden sowie die härtere Sanktionierung von Kartellrechtsverstößen durch stark gestiegene Bußgelder haben die Risiken für Unternehmen erheblich erhöht. Die Wahrscheinlichkeit der Aufdeckung eines Verstoßes ist dadurch mittlerweile sehr groß. Die Bußgelder bewegen sich inzwischen in bilanzrelevanten Größenordnungen, so dass die aufgeflogenen Kartellmitglieder erhebliche Rückstellungen für die Kartellrisiken bilden müssen.[56] Häufig verstoßen Mitarbeiter aus schlichter Unkenntnis der bestehenden Verpflichtungen gegen das Kartellrecht.

Auch das Kapitalmarktrecht ist ein Bereich, für den Compliance-Programme nach einer Gefährdungsanalyse regelmäßig eine herausragende Bedeutung haben. Eine Refinanzierung am Kapitalmarkt stellt für viele Unternehmen eine sehr wichtige Maßnahme dar, die jedoch aufgrund diverser Vorschriften, z. B. Insiderhandelsverbote oder Anzeige- und Mitteilungspflichten und den Rechtsfolgen etwaiger Verstöße überaus risikoträchtig ist. Zwar trifft die Haftung insoweit oft nur den Handelnden und nicht das Unternehmen, es droht jedoch ein empfindlicher Reputationsverlust, der eine Gefahr für den Börsenkurs des Unternehmens darstellt.

Daneben ist das Umweltrecht und das Umweltstrafrecht ein Compliance-relevanter Bereich. Diese Rechtsmaterien sind in den verschiedensten Gesetzen geregelt, die Beurteilung der Rechtslage erfordert jeweils ein ausgeprägtes Spezialwissen und birgt ein hohes Irrtumsrisiko. In diesem Bereich ist es dringend erforderlich, einen Mitarbeiter als „zentralen Umweltbeauftragten" zu ernennen, der für die jeweiligen Bereiche Fachbeauftragte bestimmt, die ihre Aktivitäten untereinander abstimmen, weiterentwickeln, Zuständigkeiten klären und Schnittstellen definieren.[57]

Ein weiteres zunehmend wichtigeres Regelungsfeld für Compliance-Aktivitäten ist die Korruptionsbekämpfung, weil die Anti-Korruptionsgesetzgebung in vielen Ländern erheblich verschärft worden ist. Jüngere Beispiele wie etwa die Fälle Volkswagen (Bestechung von Betriebsratsmitgliedern durch „Lustreisen") und Siemens (massive Korruption im Zusammenhang mit dem Einwerben von Aufträgen im Ausland) zeigen, dass neben strafrechtlichen Sanktionen oft auch erhebliche Reputationsverluste auftreten, wenn insbesondere systematische Verstöße gegen Korruptionsverbote öffentlich bekannt werden, sowie erhebliche Kosten bei der Zusammenarbeit mit Aufsichtsbehörden zur Aufklärung des Sachverhalts.

Es stellt sich die Frage, wie das Verhältnis von Risikomanagementsystemen und Compliance ist. Für eine funktionierende Compliance ist es erforderlich, zunächst unternehmensinterne Regeln und Wertestandards zu entwickeln. Im Rahmen einer Risikoanalyse müssen die gesetzlichen Anforderungen für die spezifische Unternehmenstätigkeit herausgearbeitet und Gefahrenbereiche des eigenen Unternehmens erkannt werden. Compliance erfordert insofern ein funktionierendes Risiko-

56 Lampert, Gestiegenes Unternehmensrisiko Kartellrecht – Risikoreduzierung durch Competition-Compliance-Programme, BB 2002, S. 2237.

57 Hauschka, Corporate Compliance – Unternehmensorganisatorische Ansätze zur Erfüllung der Pflichten von Vorständen und Geschäftsführern, AG 2004, 461 (470).

management, denn zwischen sonstigen Unternehmensrisiken und Compliance-Risiken besteht kein prinzipieller Unterschied. Im Hinblick auf beide Risiken muss das Unternehmen ein System einrichten, dass Gefahrenquellen analysiert, realisierte Risiken frühzeitig erkennt und Strategien zur Behandlung bereit hält. Auf der anderen Seite erfordert ein Risikomanagementsystem auch eine funktionierende Compliance. Den Mitarbeitern müssen gesetzliche Bestimmungen erläutert werden und die Einhaltung dieser Bestimmungen ist durch die Geschäftsleitung regelmäßig zu überprüfen. Von dem Standpunkt des Risikomanagers aus betrachtet, müssen Risikomanagementsysteme grundsätzlich dann eine wirksame Compliance beinhalten, wenn eine Risikoanalyse ergibt, dass ein Verstoß gegen gesetzliche Vorschriften in einzelnen Bereichen mit derart einschneidenden Rechtsfolgen sanktioniert ist, dass es ein für das Risikomanagement relevantes Risiko darstellt, das möglichst früh erkannt, an das System weitergegeben und angemessen behandelt werden muss.

Neben einer Überprüfung der Einhaltung der gesetzlichen Bestimmungen durch die Mitarbeiter sollten die Unternehmen Compliance-Programme einrichten. Hierzu zählen bestimmte Verhaltensstandards, Ethikstandards oder Corporate Governance-Grundsätze, die in internen Richtlinien an die Mitarbeiter kommuniziert werden, Schulungen, Beratung in Zweifelsfragen, die konsequente Sanktionierung von Verstößen, und unter Umständen sogar „Hotlines", bei denen Verstöße anonym gemeldet werden können. Typischerweise richten Unternehmen im Rahmen solcher Programme Compliance-Abteilungen ein und/oder bestellen Compliance-Beauftragte, die unmittelbar an die Unternehmensleitung berichten.

9. Allgemeine Organisationspflichten und Haftung

9.1 Kollektivverantwortung des Vorstands

§ 77 AktG geht von einer Kollektivverantwortung des Vorstands für die Leitung des Unternehmens aus. Durch die systematische Stellung des § 91 Abs. 2 AktG wird außerdem deutlich gemacht, dass es sich beim Risikomanagement um eine Gesamtaufgabe des Vorstands handelt. Verantwortlich für das nach § 91 Abs. 2 AktG geforderte Frühwarnsystem ist daher nicht nur das für das Risikomanagement kraft Geschäftsverteilung verantwortliche Vorstandsmitglied, sondern der Gesamtvorstand.[58] Eine Delegation des Risikomanagements wird hierdurch zwar nicht unmöglich; jedoch muss der zuständige Vorstandskollege an das Gesamtgremium berichten. Nicht zuständige Mitglieder des Vorstands müssen den zuständigen Kollegen überwachen und bei erkennbarem Fehlverhalten einschreiten. Selbstverständlich sind die einzelnen Vorstandsmitglieder für die Umsetzung des Risikomanagementsystems in ihrem Ressort sowie für dessen Einhaltung verantwortlich. Mit anderen

58 VG Frankfurt, Urteil vom 08.07.2004 – 1 E 7363/03, AG 2005, S. 265; Preußner/Zimmermann, Risikomanagement als Gesamtaufgabe des Vorstands, AG 2002, S. 657 ff.; Hauschka, Corporate Compliance – Unternehmensorganisatorische Ansätze zur Erfüllung der Pflichten von Vorständen und Geschäftsführern, AG 2004, S. 462 f.

Autorenverzeichnis

Dr. Jens-Hinrich Binder, LL.M. ist Akademischer Rat und Habilitand am Institut für Ausländisches und Internationales Privatrecht, Abt. II, Albert-Ludwigs-Universität Freiburg i. Br. Nach dem Studium der Rechtswissenschaften in Freiburg absolvierte er 2000/2001 ein Masterstudium mit dem Schwerpunkt „Banking & Finance Law" an der London School of Economics and Political Science und wurde 2004 mit einer Arbeit über rechtliche Aspekte von Bankeninsolvenzen promoviert. Seine Forschungsschwerpunkte liegen im deutschen, europäischen und internationalen Bankaufsichts-, Kapitalmarkt-, Gesellschafts- und Insolvenzrecht.

Dr. Jörg Borchert ist seit Mai 2006 Berater bei BET Büro für Energiewirtschaft und technische Planung GmbH in Aachen. Seine thematischen Schwerpunkte sind Energiehandel, Vertrieb, Kraftwerke und Risikomanagement. Nach seinem Diplom im Wirtschaftsingenieurwesen war er zuvor tätig als Analyst für Projekt- und Exportfinanzierung bei der Berliner Bank AG (1997 bis 1999), als Wissenschaftlicher Mitarbeiter an der TU Berlin am Fachgebiet für Energie- und Rohstoffwesen (1999 bis 2002, Promotion 2003), sowie als Leiter des Teams Risikomanagement Energiehandel bei der Stadtwerke Leipzig GmbH (2002 bis 2006). Seit 2002 ist er Lehrbeauftragter an der TU Berlin für die Lehrveranstaltung Energiehandel und Risikomanagement, außerdem Autor diverser Fachartikel und des Buches „Stromhandel – Institutionen, Marktmodelle, Pricing und Risikomanagement" (Schäffer-Poeschel-Verlag, 2006).

Dr. Jutta Jessenberger studierte Statistik an der Universität Dortmund und der University of Sheffield (UK). Nach Tätigkeit bei der Mars GmbH, Viersen promovierte sie an der Universität Dortmund und durchlief danach verschiedene Management Positionen bei AC Nielsen, Hamburg, und bei der OnVista AG, Köln, wo sie zuletzt als Director Content Services tätig war. Sie ist jetzt Prokuristin bei der Xerox GmbH, Black Belt und Deployment Manager für das Xerox Lean Six Sigma Programm. Außerdem ist sie verantwortlich für die Projektleitung zur Vereinheitlichung der paneuropäischen Finanzprozesse im Rahmen der Einführung eines europaweiten ERP-Systems.

Dr. Manuel Lorenz, LL.M. ist Rechtsanwalt und Partner bei Baker & McKenzie in Frankfurt/Main. Er ist außerdem als Solicitor in England und Wales zugelassen. Er leitet den Bereich Aktien- und Kapitalmarktrecht und berät bei Unternehmenstransaktionen börsennotierter Unternehmen wie z. B. Börsengängen, Übernahmen und Verschmelzungen. Daneben berät er börsennotierte Unternehmen und deren Organe im Bereich Corporate Governance und Compliance sowie in allen anderen aktien- und kapitalmarktrechtlichen Fragen. Er ist Mitherausgeber und Mitautor der

aus: Romeike (Hrsg.), Rechtliche Grundlagen des Risikomanagements.

Buchs „Deilmann/Lorenz: Die börsennotierte Aktiengesellschaft“ und Verfasser zahlreicher anderer literarischer Beiträge, vorwiegend zu aktien- und kapitalmarktrechtlichen Themen. Daneben ist er als Lehrbeauftragter am „Institute for Law and Finance“ der Johann Wolfgang Goethe-Universität in Frankfurt am Main tätig.

Dr. Thomas Münzenberg ist seit 1987 Rechtsanwalt/Strafverteidiger und Partner in der Anwaltssozietät Dr. Booz und Dr. Münzenberg in Wiesbaden. Er ist im Bereich Wirtschaftsstrafrecht tätig und betreut forensisch, beratend und im Rahmen von Fortbildungsmaßnahmen Unternehmen sowie deren Organe und leitende Angestellte. Dabei vertritt er den zuletzt genannten Personenkreis nicht nur im Bereich der Strafverteidigung, sondern auch im Bereich zivilrechtlicher Haftungsprozesse. Dr. Münzenberg ist Mitglied des Arbeitskreises „Externe und Interne Überwachung der Unternehmung“ der Schmalenbach-Gesellschaft.

Frank Romeike ist Vorstand der Risk Management Association (e.V.) sowie Geschäftsführer der RiskNET GmbH. RiskNET ist das führende deutschsprachige Informationsportal rund um den Themenkomplex Risikomanagement und Compliance und wird monatlich von etwa 160.000 bis 200.000 Risikomanagern, Wirtschaftsprüfern, Controllern, Unternehmensberatern und Geschäftsführern gelesen. Er ist außerdem Chefredakteur der „Zeitschrift für Risk, Fraud & Governance“, die beim Erich Schmidt Verlag (Berlin) erscheint sowie verantwortlicher Chefredakteur der Zeitschrift „Risiko Manager“, die beim Bank-Verlag (Köln) erscheint. Zuvor war er Risikomanager bei der IBM Central Europe, wo er u. a. an der Implementierung des weltweiten Risikomanagement-Prozesses der IBM beteiligt war und mehrere internationale Projekte leitete.

Prof. Dr. Hans-Peter Schwintowski ist Geschäftsführender Direktor des Instituts für Energie- und Wettbewerbsrecht in der Kommunalen Wirtschaft e.V. an der Humboldt-Universität zu Berlin. Seine Arbeitsschwerpunkte sind Energierecht, Privatversicherungsrecht, Bank- und Kapitalmarktrecht, Wettbewerbs- und Kartellrecht, Europäisches Wirtschaftsrecht, Gesellschafts- und Konzernrecht, Handelsrecht, Rechtstheorie und Rechtsvergleichung.

Dr. Peter Winter ist wissenschaftlicher Mitarbeiter am Lehrstuhl für Allgemeine Betriebswirtschaftslehre und Industrie, insbesondere Produktionswirtschaft und Controlling der Universität Mannheim. Er promovierte an der Universität Mannheim über Risikocontrolling in Nicht-Finanzunternehmen und hat zahlreiche Fachbeiträge zu Risikomanagement und -controlling veröffentlicht.

Gundolf Zimmermann studierte Wirtschaftswissenschaft an der Ruhr-Universität Bochum. Nach Tätigkeiten bei Arthur Andersen GmbH und Merckle/ratiopharm GmbH war er zuletzt bis 2001 Tax Manager bei der Wal-Mart Germany GmbH & Co KG. Er ist jetzt Prokurist und als Chief Accountant der Xerox GmbH verantwortlich für die Bereiche Rechnungswesen und Steuern. Außerdem leitete er in den Jahren 2003 und 2004 die Einführung des internen Kontrollsystems nach Section 404 des Sarbanes-Oxley Acts in Deutschland, das derzeit als Benchmark innerhalb des europäischen Konzerns gilt.

Risiken managen: aktuelle Rechtsgrundlagen auf einen Blick

Manager und Aufsichtsorgane sehen sich immer stärker umzingelt von Rechtsvorschriften zum Risikomanagement – mit enormen Konsequenzen für persönliche Haftung und strafrechtliche Sanktionen.

Informieren Sie sich rechtzeitig!

Frank Romeike und weitere Experten bündeln in diesem Buch erstmals die relevanten rechtlichen Grundlagen zum Risikomanagement. Sie erfahren, wie Sie in der Praxis den zahlreichen Compliance-Anforderungen begegnen:

- nationale und internationale gesetzliche Grundlagen des Risikomanagements
- Corporate Governance, Compliance und Business Judgment Rule
- Standards im Risikomanagement
- Straf- und Zivilrecht sowie Haftung der Unternehmensleitung und -aufsicht
- Branchenwissen: Banken und Finanzdienstleister, Versicherungen, Industriekonzerne, Energieunternehmen.

Mit diesem Leitfaden gestalten Sie die Risikoprävention wirkungsvoll und schalten hohe Haftungspotenziale und Sanktionsrisiken im Vorfeld aus!

Leseprobe, mehr zum Buch unter ESV.info/978 3 503 10647 9

9 783503 106479
€(D) 49,95

www.ESV.info