Keywords: *Rechtliche Grundlagen*
KonTraG
Corporate Governance

Rechtliche Grundlagen des Risikomanagements

Juristische Rahmenbedingungen für den Aufbau und die Ausgestaltung von Risikomanagementsystemen in deutschen Unternehmen

Dr. Manuel Lorenz, LL.M*

Der Beitrag erläutert die rechtlichen Grundlagen, aus denen sich für die Organe einer Kapitalgesellschaft mit Sitz in Deutschland die Verpflichtung ergibt, ein Risikomanagementsystem einzurichten und zu betreiben, sowie, welche rechtlichen Mindestanforderungen für die Ausgestaltung eines solchen Systems gelten.

Als zentrales Element des Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) wurde im Jahr 1998 durch den neu geschaffenen § 91 Abs. 2 AktG für Aktiengesellschaften die Pflicht zur Schaffung eines Überwachungssystems für bestandsgefährdende Entwicklungen gesetzlich verankert. Weitere Normen des KonTraG beschäftigen sich mit der Risikoberichterstattung im Jahresabschluss und der Überprüfung durch die Abschlussprüfer.

Das KonTraG ist aber nicht die einzige Rechtsquelle für das Risikomanagement. Nachstehend werden auch die Normen angesprochen, die eine Ausstrahlungswirkung für die Auslegung der Vorschriften des KonTraG haben. Abschließend wird dargestellt, wie Haftungsregelungen die Ausgestaltung und Anwendung eines Risikomanagementsystems beeinflussen.

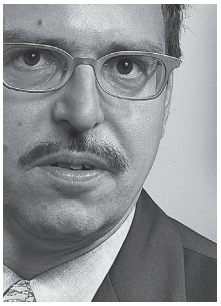
1. Das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich

1.1 § 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 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.


Dr. Manuel Lorenz

Auffällig an der Vorschrift ist, dass keine ausdrückliche Pflicht begründet wird, ein umfassendes Risikomanagementsystem einzurichten. Angesprochen wird von der Vorschrift allenfalls eine Komponente eines Risikomanagementsystems, nämlich die Einrichtung eines Überwachungssystems zur Früherkennung von bestandsgefährdenden Entwicklungen. Nicht einmal der Begriff „Risiken" wird im Gesetz verwendet, sondern nur der Begriff „Entwicklungen".[1] Wie der Vorstand mit erkannten bestandsgefährdenden Risiken oder Entwicklungen umgeht, wird in § 91 Abs. 2 AktG nicht explizit geregelt. Freilich ergibt sich aus den allgemeinen Sorgfalts- und Organisationspflichten, dass ein Vorstand nicht tatenlos bleiben kann, wenn ihm durch das Frühwarnsystem bestandsgefährdende Entwicklungen (oder Risiken) gemeldet werden. Vielmehr muss er sich in solchen Fällen fragen, wie man mit diesen Risiken umgeht. Dafür bietet sich die Einrichtung eines umfassenden Risikomanagementsystems an.

In der Literatur herrschen beträchtliche Meinungsunterschiede über die Frage, ob sich aus § 91 Abs. 2 AktG die Pflicht zur Einrichtung eines solchen vollwertigen Risikomanagementsystems ergibt.[2] Der Streit hat eine geringe praktische Bedeutung, denn wie nachfolgend noch gezeigt wird, lässt sich die Pflicht zur Einrichtung eines Risikomanagementsystems auch aus weiteren Vorschriften ableiten. Daher dürfte ein etwa verbleibendes Leitungsermessen des Vorstandes, ob er ein solches System einführen will oder nicht, beträchtlich eingeschränkt sein.

1.2 Prüfung des Frühwarnsystems

§ 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 Überwachungssystem seine Aufgaben erfüllen kann. Es findet also über die Abschlussprüfung nicht nur eine Kontrolle der Existenz des Frühwarnsystems statt, sondern das System ist auch auf seine Funktionalität zu überprüfen. Hierfür existiert bei den Wirtschaftsprüfern ein eigener Prüfstandard (IDW PS 340)[3]. Aus dem Inhalt des

* Dr. Manuel Lorenz ist Partner in der internationalen Anwaltssozietät Baker & McKenzie. Er ist im Bereich Kapitalmarkt- und Aktienrecht tätig. Neben der Betreuung von Kapitalmarkttransaktionen, wie etwa Börsengängen und Übernahmen berät er häufig Unternehmensorgane in Fragen der Corporate Governance und Compliance, einschließlich des Risikomanagements.

1 Hinweis auch bei Seibert, Die Entstehung des § 91 Abs. 2 AktG im KonTraG, in Festschrift für Bezzenberger 2000, S. 437, wonach fortlaufende Entwicklungen und nicht abstrakte oder latente Risiken gemeint seien.

2 Dagegen: Seibert, Die Entstehung des § 91 Abs. 2 AktG im KonTraG, in Festschrift für Bezzenberger 2000, S. 437, Hüffer, Aktiengesetz, 6. Auflage 2004, § 91 Rn. 9 mit Nachweis des Meinungsstandes.

3 Abgedruckt in WpP 1999, S. 658 ff.

Der DCGK umfasst eine Reihe von Regelungen, die sich mit dem Risikomanagement befassen.

Prüfstandards lassen sich auch Rückschlüsse auf die Ausgestaltung des Früherkennungssystems ziehen. Insbesondere stellt PS 340 klar, dass zur Erkennung bestandsgefährdender Entwicklungen ein Risikofrüherkennungssystem einzurichten ist.[4] Auch wenn die Prüfpflicht nur für börsennotierte Unternehmen besteht, kann man aus dem Prüfstandard Anforderungen an ein entsprechendes System für nicht börsennotierte Aktiengesellschaften entnehmen.

1.3 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, werden in erster Linie Finanzinstrumente erfasst, vor allem Hedge-Geschäfte in Form von Derivaten. Zumindest in diesem Bereich verlangt das Gesetz nicht nur eine Darstellung der Risiken, sondern eben auch Angaben zu den Risikomanagementzielen 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.

Zukünftig dürfte allerdings aus europarechtlichen Gründen die Darstellung im Lagebericht deutlich ausführlicher ausfallen und sich auch auf ein allgemeines Risikomanagementsystem erstrecken. Der Vorschlag zur Änderung der Richtlinie 78/660/EWG vom 27.10.2004[5] sieht die Aufnahme eines so genannten „Corporate Governance Statements" vor, das u. a. eine Beschreibung der internen Kontroll- und Risikomanagementsysteme der Gesellschaft enthalten muss.

Theoretisch ist sowohl nach dem Richtlinienvorschlag, als auch nach dem HGB im Bezug auf Absicherungsgeschäfte vorstellbar, dass der Lagebericht an dieser Stelle eine Negativerklärung enthält, dass Risikomanagementsysteme nicht vorhanden sind. Hinter solchen Vorschriften verbirgt sich indes die Annahme, dass eine Gesellschaft üblicherweise über solche Instrumentarien verfügen muss. Die genannten Vorschriften sind daher Indikatoren dafür, dass die Rechtsordnung allgemein von der Existenz von Risikomanagementsystemen als Teil einer „Best Practice" ausgeht.

2. Deutscher Corporate Governance Kodex

Der deutsche Corporate Governance Kodex (DCGK)[6] beinhaltet eine Reihe von Regelungen, die sich mit dem Risikomanagement befassen.

2.1 Zielsetzung und Wirkungsweise des DCGK

Der DCGK enthält ausweislich seiner Präambel 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 Unternehmensführung darzustellen. Nur wenn der Kodex das Wort „soll" verwendet, handelt es sich um ein 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.[7]

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. Abwei-

4 Vgl. WpP 1999, S. 658.
5 Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Abänderung der Richtlinien 78/660/EWG und 83/349/EWG hinsichtlich der Jahresabschlüsse bestimmter Arten von Unternehmen und konsolidierter Abschlüsse; KOM (2004) 725 im Hinblick auf die Aufnahme eines neuen Art. 46a in die Richtlinie 78/660.
6 Abrufbar unter http://www.corporate-governance-code.de
7 Vgl. Präambel zum Deutschen Corporate Governance-Kodex (geltende Fassung vom 2. Juni 2005).

Kreditinstitute und Finanzdienstleister unterliegen einer strengen Regulierung.

chungen von Anregungen des DCGK müssen nicht offen gelegt werden.

2.2 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 spiegeln lediglich den geltenden Rechtszustand wider. In Ziffer 4.1.4 DCGK heißt es in einer sehr allgemeinen Form:

„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."

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.

3. 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 2 KWG bestimmt, dass eine ordnungsgemäße Geschäftsorganisation insbesondere umfasst:

„Angemessene interne Kontrollverfahren, die aus einem internen Kontrollsystem und einer internen Revision bestehen; das interne Kontrollsystem umfasst insbesondere geeignete Regelungen zur Steuerung und Überwachung der Risiken."

Zur näheren Konkretisierung hat die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) als zuständige Behörde vor kurzem zusammengefasste „Mindestanforderungen an das Risikomanagement – MaRisk" erlassen[8], die die bisherigen Mindestanforderungen zum Kreditgeschäft (MaK) und zum Handelsbuchgeschäft (MaH) zusammenfassen, straffen und flexibilisieren, aber zum allgemeinen Risikomanagement auch neue Verpflichtungen formulieren.

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 Szenariobetrachtungen berichten zu lassen, wobei in die Risikoberichterstattung bei Bedarf auch Handlungsvorschläge zur Risikoreduzierung aufzunehmen sind. 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.

Der allgemeine Teil der MaRisk ist weitgehend auch auf Unternehmen anderer Branchen übertragbar. Insofern ist die Frage berechtigt, 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. Neben verschiedenen Äußerungen in der Literatur[9] zu diesem Thema hat sich in jüngerer Zeit auch ein Gericht für eine solche Ausstrahlungswirkung ausgesprochen. In einer Entscheidung des Verwaltungsgerichts Frankfurt am Main[10] wurde für ein Versicherungsunternehmen über die Vorschrift des § 91 Abs. 2 AktG der § 25a Abs. 1 KWG zur Auslegung herangezogen. Das Gericht führt aus, dass der Gesetzgeber bei der Einführung des § 91

8 Abrufbar auf der Webseite der BaFin unter www.bafin.de, Rechtliche Grundlagen – Verlautbarungen und Rundschreiben – Rundschreiben 2005.

9 Vor allem Preußner/Zimmermann, Risikomanagement als Gesamtaufgabe des Vorstands, AG 2002, S. 657 ff., insb. S. 659 f.; Preußner, Risikomanagement im Schnittpunkt von Bankaufsichtsrecht und Gesellschaftsrecht, NZG 2004, S. 7 ff., insb. 59 f., Fleischer, Zur Leitungsaufgabe des Vorstands im Aktienrecht, ZIP 2003, S. 1 ff.

10 VG Frankfurt, Urteil vom 8.7.2004 – 1 E 7363/03, AG 2005, S. 264.

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.[11]

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[12] von einer Pflichtenidentität von § 25a KWG und § 91 Abs. 2 AktG aus.

Auch wenn es damit noch nicht „Allgemeingut" 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.

4. Die neue Baseler Eigenkapitalvereinbarung (Basel II)

Die als „Basel II" bekannt gewordenen Vorschriften zur Eigenkapitalunterlegung in Banken sind zwar zunächst nur für Kreditinstitute verbindlich. Allerdings setzen diese neuen Regularien auch mittelbare Normen, die das Risikomanagement von Unternehmen allgemein betreffen. Nach diesen Vorschriften, die über eine EU-Richtlinie auch Gesetz in allen europäischen Ländern werden, sind die Banken verpflichtet, bei der Kreditvergabe ein Rating ihrer Kunden vorzunehmen. Ein nicht unwesentlicher Teil der Kreditratings wird auch davon abhängen, welche Risikomanagementmaßnahmen im Unternehmen getroffen wurden. Die Anforderungen der Banken oder Ratingagenturen bei der Festelegung des Ratings werden zukünftig einen weiteren Standard für ein Risikomanagementsystem setzen. Die allgemeinen Pflichten des Vorstands werden es deshalb zukünftig gebieten, zur Rating-Verbesserung Risikomanagementsysteme einzuführen oder zu optimieren.

5. Allgemeine Organisationspflichten und Haftung

5.1 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 Vorstandes handelt. Verantwortlich für das nach § 91 Abs. 2 AktG geforderte Frühwarnsystem íst daher nicht nur das für das Risikomanagement kraft Geschäftsverteilung verantwortliche Vorstandsmitglied, sondern der Gesamtvorstand.[13] 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 Worten muss jedes Vorstandsmitglied die in seinem eigenen Ressort vorkommenden Risiken beherrschen.[14]

5.2 Organisationspflichten

In einem arbeitsteilig organisierten Unternehmen wird eine Beherrschung des Risikos, wie bereits Eingangs erwähnt, nur möglich sein, wenn dies durch eine entsprechende Unternehmensorganisation sichergestellt ist. In einem großen Unternehmen muss die Unternehmensleitung auf viele Schultern verteilt werden. Hierdurch werden Leitungsaufgaben in die zweite, dritte oder sogar noch tiefere Managementebene verlagert. Kein Vorstand kann jeden Mitarbeiter ständig bei seiner Aufgabenerfüllung überwachen. Die Rechtsprechung erkennt dies zwar durchaus an, kompensiert das hierdurch eintretende größere Schädigungsrisiko indes durch eine Organisationspflicht. Damit haften Vorstandsmitglieder zwar nicht für jedes Verschulden eines Mitarbeiters, aber für die Einrichtung einer Organisation, die zumindest bei systemgemäßem Funktionieren eine Schädigung ausschließt.[15]

---

11 VG Frankfurt, Urteil vom 8.7.2004 – 1 E 7363/03, AG 2005, S. 265.

12 LG Berlin, Urteil vom 3.7.2002 – 2 O 358/01, AG 2002, 682ff, kommentiert von Preußner/Zimmermann, Risikomanagement als Gesamtaufgabe des Vorstands, AG 2002, S. 657 ff.

13 VG Frankfurt, Urteil vom 8.7.2004 – 1 E 7363/03, AG 2005, S. 265; Preußner/Zimmermann, Risikomanagement als Gesamtaufgabe des Managements, AG 2002, S. 657 ff.; Hauschka, Corporate Compliance – Unternehmensorganisatorische Ansätze zur Erfüllung der Pflichten von Vorständen und Geschäftsführern, AG 2004, S. 462 f.

14 Semler/Peltzer, Arbeitshandbuch für Vorstandsmitglieder, § 1 Rn. 236.

15 Ausführlich zu Strategien zur Haftungsvermeidung Hauschka, Corporate Compliance – Unternehmensorganisatorische Ansätze zur Erfüllung der Pflichten von Vorständen und Geschäftsführern, AG 2004, S. 462 f.

Risikomanagement ist eine rechtliche Pflicht und keine unternehmerische Entscheidung.

Eine solche Organisation besteht im Regelfall aus einem System von internen Anweisungen und einer Kontrolle, ob die internen Anweisungen auch eingehalten werden, zumindest stichprobenartig. Befasst sich der Vorstand also nicht allein mit dem Risikomanagement, muss er eine entsprechende Risikomanagement-Organisation durch unternehmensinterne Richtlinien und die Kontrolle von deren Einhaltung schaffen.

5.3 Haftung für fehlerhaftes Risikomanagement?

Es verbleibt die Frage, wie sich ein fehlendes oder mangelhaftes Risikomanagementsystem auf die konkrete Haftung der Unternehmensorgane auswirkt. Jede Haftung setzt zunächst die Entstehung eines Schadens beim Unternehmen voraus. Ein mangelndes oder mangelhaftes Risikomanagementsystem ist als solches kein Schaden. Jedoch können Schäden aus mangelhaftem Risikomanagement dann entstehen, wenn es als Folge zu unternehmerischen Fehlentscheidungen kommt, die ihrerseits einen Schaden beim Unternehmen auslösen oder wenn die Gesellschaft durch ein von außen eintretendes Ereignis geschädigt wurde, auf dessen Eintritt sie nicht oder schlecht vorbereitet war.

Eine Haftung setzt neben der Entstehung eines Schadens voraus, dass der Vorstand eine Pflicht verletzt und der Vorstand nicht sorgfältig gehandelt hat, wobei der Vorstand die Beweislast dafür trägt, dass er sorgfältig gehandelt hat (§ 93 Abs. 2 AktG).

Weil Unternehmensleiter täglich unternehmerische Entscheidungen zu treffen haben, bei der sie die unternehmerischen Chancen und Risiken gegeneinander abwägen müssen, wäre es allerdings unangebracht und kontraproduktiv, müssten Vorstandsmitglieder immer dann haften, wenn sich eine unternehmerische Entscheidung im nachhinein als falsch herausstellt, insbesondere, wenn sich ein bewusst eingegangenes Risiko materialisiert. Deswegen haben die Gerichte – in Anlehnung an amerikanische Rechtsprechung – die so genannte Business Judgment Rule geschaffen.[16] Im Gesetz zur Unternehmensintegrität und Modernisierung des Anfechtungsrechts (UMAG) wurde die Business Judgment Rule nunmehr in § 93 Abs. 1 AktG wie folgt kodifiziert:

„Eine Pflichtverletzung liegt nicht vor, wenn das Vorstandsmitglied bei einer unternehmerischen Entscheidung vernünftigerweise annehmen dürfte, auf der Grundlage angemessener Information zum Wohl der Gesellschaft zu handeln."

Mangelhaftes Risikomanagement dürfte häufig Ursache für die Fehlbeurteilung oder fehlerhafte Behandlung von Risiken im Rahmen von unternehmerischen Entscheidungen sein. Aus der Business Judgment Rule lassen sich folgende Schlussfolgerungen im Bezug auf die Einrichtung und den Betrieb eines Risikomanagementsystems ableiten:

- Risikomanagement ist keine unternehmerische Entscheidung, sondern eine rechtliche Pflicht, wie sich aus den vorangegangenen Ausführungen ergibt. Das Fehlen jeglichen Risikomanagements kann daher nicht mit der Business Judgment Rule gerechtfertigt werden. Diese ist hierfür nicht anwendbar.
- Besteht dagegen ein Risikomanagementsystem, so ist die Business Judgment Rule grundsätzlich anwendbar, wenn Auslöser für den konkreten Schadensfall eine unternehmerische Entscheidung war.
- Ob sich das Vorstandsmitglied in dieser Situation auf die Business Judgment Rule berufen kann, hängt aber auch von der Qualität des Systems ab. Dass der Vorstand vernünftigerweise annehmen durfte, auf der Basis ausreichender Informationen zu handeln, setzt voraus, dass sich der Vorstand auf die Risikoerkennung, also auf das Frühwarnsystem verlassen konnte. Ist das Frühwarnsystem nach § 91 Abs. 2 AktG mangelhaft, wird der Vorstand häufig nicht annehmen können, dass er auf der Basis ausreichender Informationen gehandelt hat.
- In ähnlicher Weise werden Mängel des Risikomanagementsystems im Bereich der Risikobewertung, der Risikosteuerung oder -bewältigung häufig dazu führen, dass der Vorstand nicht vernünftigerweise annehmen kann, zum Wohl der Gesellschaft zu handeln. Insbesondere, wenn dem Vorstand bewusst ist, dass das System nur mangelhafte Daten zur Bewertung und Steuerung von Risiken liefert, kann er sich nicht darauf verlassen, dass seine Entscheidung bei der Abwägung der unternehmerischen Chancen und Risiken auch aus der ex ante-Sicht richtig ist.

6. Schlussfolgerungen für die Ausgestaltung eines Risikomanagementsystems für Unternehmensleiter

Die Anforderungen an ein Risikomanagementsystem sind grundsätzlich unternehmensspezifisch und hängen von der Größe des Unternehmens sowie von der Höhe und Zahl der Risiken ab. Die konkreten Anforderungen an ein Risikomanagementsystem werden durch die Ausstrahlungswirkung der bereits oben erörterten Vorschriften beeinflusst. Das Management ist deshalb gut beraten, die Anforderungen an die Dokumentation im Jahresabschluss, den Prüfstandard der Wirtschaftsprüfer, den deutschen Corporate Governance Kodex und auch das Bankaufsichtsrecht, insbesondere die MaRisk, heranzuziehen, und zu überprüfen, ob das eingerichtete Risikomanagementsystem diesen Anforderungen genügt.

16 Wegweisend ist die Entscheidung ARAG/Garmenbeck, BGH, Urteil vom 21.4.1997, Az. II ZR 175/95, BGHZ 135, 244, 253.

Aus dem einzurichtenden Früherkennungssystem muss sich ein Katalog aller wesentlichen das Unternehmen berührenden Risiken entwickeln lassen. Diese Risiken sind in Bezug auf ihre Eintrittswahrscheinlichkeit und die denkbaren Auswirkungen auf das Unternehmen zu bewerten.

Mit Hilfe entsprechender Verfahren sollte die Risikotragfähigkeit des Unternehmens, ausgehend vom verfügbaren Eigenkapital bestimmt und mit den bewerteten Risiken in Bezug gesetzt werden. So kann erkannt werden, ob sich „bestandsgefährdende Entwicklungen" i.S.d. § 91 Abs. 2 AktG für das Unternehmen abzeichnen. Es müssen Verfahren entwickelt werden, die den Umgang mit den Risiken regeln und sicherstellen, dass die Risikotragfähigkeit des Unternehmens nicht überschritten wird.

Wichtig ist, im Unternehmen ein Gremium zu schaffen, dass sich mit den Risiken befasst, beispielsweise ein Risikoausschuss. In das Risikomanagementsystem bzw. den Risikoausschuss müssen sowohl das Controlling (für die Informationsbeschaffung, Aufbereitung und Weiterleitung an den Vorstand) und die interne Revision (Prüfung der inhaltlichen Richtigkeit der Daten und des Systems) eingebunden werden.

Sowohl die Risiken selbst, als auch die Risikosteuerung muss intern (Richtlinien für die Mitarbeiter) und extern (Risikoberichterstattung im Jahresabschluss) kommuniziert werden. Intern bietet sich beispielsweise ein Risikohandbuch als Kommunikationsmittel an.

7. Rolle des Aufsichtsrates

Auch der Aufsichtsrat ist in das Risikomanagement eingebunden. Eine „Best Practice" gibt der DCGK vor. Der Aufsichtsrat muss sicherstellen, dass der Vorstand seinen Berichtspflichten zum Risikomanagement nach Ziffer 3.4 Abs. 2 DCGK in Verbindung mit § 90 AktG nachkommt. Der Aufsichtsratsvorsitzende hat gemäß Ziffer 5.2 Abs. 3 DCGK regelmäßig das Risikomanagement mit dem Vorstand zu beraten und der Aufsichtsrat sollte sich im Prüfungsausschuss mit dem Thema Risikomanagement eingehend beschäftigen.

Bereits aus allgemeinen Normen ergibt sich darüber hinaus ein weiterer Pflichtenkatalog des Aufsichtsrats. Kraft seiner Pflicht zur Überwachung des Vorstands ist der Aufsichtsrat nämlich originärer Risikomanager im Bezug auf das Personalrisiko des Vorstandes (§ 111 AktG). Aus § 111 AktG ergibt sich außerdem eine allgemeine Pflicht zur Überwachung der Tätigkeit des Vorstandes, also auch in Bezug auf das Risikomanagement, insbesondere die Einrichtung des Systems nach § 91 Abs. 2 AktG, sowie die Erfassung, Bewertung und Steuerung der Risiken durch den Vorstand.[17] Dabei muss der Aufsichtsrat (bzw. der Prüfungsausschuss) das Risikomanagementsystem beurteilen. Er muss sich insbesondere hinsichtlich des Vorhandenseins des Systems vergewissern und es bewerten.[18] Hinsichtlich der Rechtmäßigkeit des Systems (also der Erfüllung der gesetzlichen Anforderungen) verbleibt dem Aufsichtsrat dabei kein Ermessensspielraum.[19] Dieser kann sich allenfalls auf die Zweckmäßigkeit und Wirtschaftlichkeit des Risikomanagementsystems erstrecken.

Bei der Beurteilung des Risikomanagementsystems sollte sich der Aufsichtsrat auf die interne Revision und den Abschlussprüfer stützen. Insbesondere ist es dem Aufsichtsrat möglich, durch entsprechende Ausgestaltung des Prüfungsauftrags das System auch vom Abschlussprüfer besonders in Augenschein nehmen zu lassen.[20]

Stellt der Aufsichtsrat Mängel fest, hat er diese gegenüber dem Vorstand zu beanstanden. Darüber hinaus sollte der Aufsichtsrat auch im Rahmen seiner Berichterstattung an die Hauptversammlung über seine Tätigkeiten im Bezug auf die Überwachung des Risikomanagements des Vorstands eingehen.[21]

8. Fazit

Angesichts der juristischen Anforderungen und der Haftungsrisiken kann es sich kein Unternehmensleiter leisten, das Risikomanagement zu vernachlässigen. Dies betrifft nicht nur die Vorstände von Aktiengesellschaften (börsennotiert oder nicht), sondern auch die entsprechenden Organe anderer Unternehmensformen.

Die zunehmende Dichte der Normen, die sich mit Risikomanagement befassen und die potenzielle Ausstrahlungswirkung vieler Vorschriften auf die Verpflichtungen der Unternehmensorgane, führen dazu, dass die Anforderungen an die Ausgestaltung des Risikomanagementsystems stetig steigen.

Der Aufsichtsrat ist in das Risikomanagement eingebunden und trägt in diesem Bereich auch ein eigenes Haftungsrisiko.

---

17 Claussen/Korth, Anforderungen an ein Risikomanagementsystem aus der Sicht des Aufsichtsrates, Festschrift für Lutter, 2000, S.329 f.; Feddersen, Überwachung durch den Aufsichtsrat, Handbuch Corporate Governance, S. 464.

18 Claussen/Korth, Anforderungen an ein Risikomanagementsystem aus der Sicht des Aufsichtsrates, Festschrift für Lutter, 2000, S.330 ff.; Feddersen, Überwachung durch den Aufsichtsrat, Handbuch Corporate Governance, S. 464.

19 Hierzu auch Schichold, Die Überwachung des Risikomanagement-Systems durch den Aufsichtsrat eine Aktiengesellschaft, Festschrift für Strobel, 2001, S. 418.

20 Vgl. Schichold, Die Überwachung des Risikomanagement-Systems durch den Aufsichtsrat eine Aktiengesellschaft, Festschrift für Strobel, 2001, S. 408 ff.

21 Vgl. Schichold, Die Überwachung des Risikomanagement-Systems durch den Aufsichtsrat eine Aktiengesellschaft, Festschrift für Strobel, 2001, S. 420 f.