

Der Open-Access-Publikationsserver der ZBW – Leibniz-Informationzentrum Wirtschaft  
*The Open Access Publication Server of the ZBW – Leibniz Information Centre for Economics*

Pampel, Katrin

Working Paper

## Anforderungen an ein betriebswirtschaftliches Risikomanagement unter Berücksichtigung nationaler und internationaler Prüfungsstandards

Wismarer Diskussionspapiere, No. 13/2005

**Provided in cooperation with:**

Hochschule Wismar

Suggested citation: Pampel, Katrin (2005) : Anforderungen an ein betriebswirtschaftliches  
Risikomanagement unter Berücksichtigung nationaler und internationaler Prüfungsstandards,  
Wismarer Diskussionspapiere, No. 13/2005, <http://hdl.handle.net/10419/23322>

**Nutzungsbedingungen:**

Die ZBW räumt Ihnen als Nutzerin/Nutzer das unentgeltliche, räumlich unbeschränkte und zeitlich auf die Dauer des Schutzrechts beschränkte einfache Recht ein, das ausgewählte Werk im Rahmen der unter

→ <http://www.econstor.eu/dspace/Nutzungsbedingungen>  
nachzulesenden vollständigen Nutzungsbedingungen zu vervielfältigen, mit denen die Nutzerin/der Nutzer sich durch die erste Nutzung einverstanden erklärt.

**Terms of use:**

*The ZBW grants you, the user, the non-exclusive right to use the selected work free of charge, territorially unrestricted and within the time limit of the term of the property rights according to the terms specified at*

→ <http://www.econstor.eu/dspace/Nutzungsbedingungen>  
*By the first use of the selected work the user agrees and declares to comply with these terms of use.*



**Hochschule Wismar**

University of Technology, Business and Design

**Fachbereich Wirtschaft**



**Hochschule Wismar**

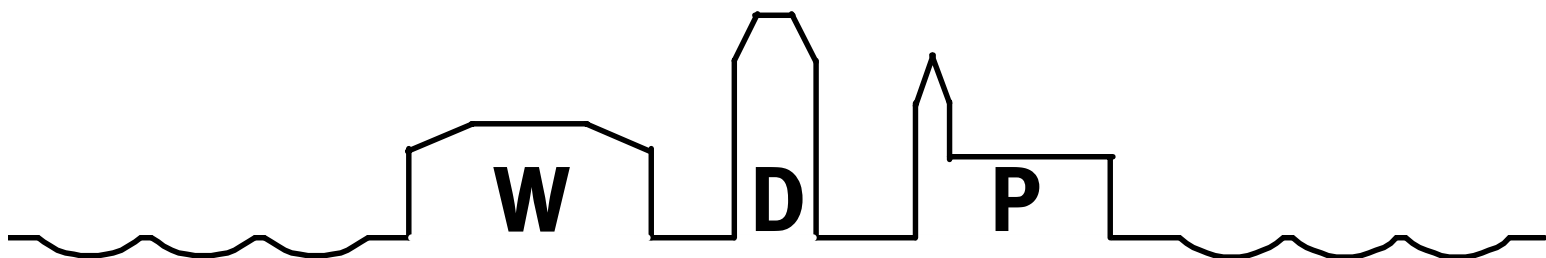
University of Technology, Business and Design

**Faculty of Business**

Katrin Pampel

Anforderungen an ein betriebswirtschaftliches Risiko-  
management unter Berücksichtigung nationaler und in-  
ternationaler Prüfungsstandards

Heft 13 / 2005



**Wismarer Diskussionspapiere / Wismar Discussion Papers**

Der Fachbereich Wirtschaft der Hochschule Wismar, University of Technology, Business and Design bietet die Präsenzstudiengänge Betriebswirtschaft, Management sozialer Dienstleistungen, Wirtschaftsinformatik und Wirtschaftsrecht sowie die Fernstudiengänge Betriebswirtschaft, International Management, Krankenhaus-Management und Wirtschaftsinformatik an. Gegenstand der Ausbildung sind die verschiedenen Aspekte des Wirtschaftens in der Unternehmung, der modernen Verwaltungstätigkeit im sozialen Bereich, der Verbindung von angewandter Informatik und Wirtschaftswissenschaften sowie des Rechts im Bereich der Wirtschaft.

Nähere Informationen zu Studienangebot, Forschung und Ansprechpartnern finden Sie auf unserer Homepage im World Wide Web (WWW): <http://www.wi.hs-wismar.de/>.

Die Wismarer Diskussionspapiere/Wismar Discussion Papers sind urheberrechtlich geschützt. Eine Vervielfältigung ganz oder in Teilen, ihre Speicherung sowie jede Form der Weiterverbreitung bedürfen der vorherigen Genehmigung durch den Herausgeber.

Herausgeber: Prof. Dr. Jost W. Kramer  
Fachbereich Wirtschaft  
Hochschule Wismar  
University of Technology, Business and Design  
Phillipp-Müller-Straße  
Postfach 12 10  
D – 23966 Wismar  
Telefon: ++49/(0)3841/753 441  
Fax: ++49/(0)3841/753 131  
e-mail: [j.kramer@wi.hs-wismar.de](mailto:j.kramer@wi.hs-wismar.de)

Vertrieb: HWS-Hochschule Wismar Service GmbH  
Phillipp-Müller-Straße  
Postfach 12 10  
23952 Wismar  
Telefon: ++49/(0)3841/753-574  
Fax: ++49/(0)3841/753-575  
e-mail: [info@hws-startupfuture.de](mailto:info@hws-startupfuture.de)  
Homepage: [www.hws-startupfuture.de](http://www.hws-startupfuture.de)

ISSN 1612-0884

ISBN 3-910102-69-7

JEL-Klassifikation M41, M21

Alle Rechte vorbehalten.

© Hochschule Wismar, Fachbereich Wirtschaft, 2005.

Printed in Germany

## **Inhaltsverzeichnis**

|   |           |
|---|-----------|
| <b>Vorwort</b>  | <b>5</b>  |
| <b>1. Einleitung</b>  | <b>6</b>  |
| <b>2. Risikobegriff</b>   | <b>7</b>  |
| <b>3. Risikoarten und -kategorisierung</b>                                    | <b>10</b> |
| <b>4. Begriff und Ziele des Risikomanagements</b>                             | <b>13</b> |
| 4.1. Entstehung des Begriffs „Risikomanagement“                               | 13        |
| 4.2. Ziele des Risikomanagements  | 14        |
| <b>5. Betriebswirtschaftliche Anforderungen an ein Risikomanagementsystem</b> | <b>15</b> |
| 5.1. Risikomanagementprozess  | 15        |
| 5.1.1. Festlegung der Risikostrategie   | 15        |
| 5.1.2. Risikoidentifikation   | 18        |
| 5.1.3. Risikoanalyse und -bewertung   | 22        |
| 5.1.4. Risikokommunikation  | 25        |
| 5.1.5. Risikosteuerung  | 26        |
| 5.1.6. Risikoüberwachung  | 31        |
| 5.2. Risikocontrolling  | 31        |
| <b>6. Externe Anforderungen an ein Risikomanagement</b>                       | <b>33</b> |
| 6.1. Nationale Anforderungen  | 35        |
| 6.1.1. „Risikomanagement“ gemäß KonTraG                                       | 38        |
| 6.1.1.1. Risikofrüherkennungs- und Überwachungssystem                         | 39        |
| 6.1.1.1.1. Anwendungsbereich  | 39        |
| 6.1.1.1.2. Inhalt   | 40        |
| 6.1.1.2. Risikoberichterstattung  | 46        |
| 6.1.1.2.1. Anwendungsbereich  | 47        |
| 6.1.1.2.2. Inhalt   | 47        |
| 6.1.1.3. Prüfung des Risikofrüherkennungs- und Überwachungssystems            | 53        |
| 6.1.1.3.1. Anwendungsbereich  | 53        |
| 6.1.1.3.2. Inhalt   | 54        |
| 6.1.2. „Risikomanagement“ gemäß IDW PS 340                                    | 56        |

|            |   |           |
|------------|---|-----------|
| 6.1.2.1.   | Komponenten des „Risikomanagements“   | 56        |
| 6.1.2.1.1. | Festlegung der Risikofelder   | 57        |
| 6.1.2.1.2. | Risikoerkennung und Risikoanalyse   | 58        |
| 6.1.2.1.3. | Risikokommunikation   | 58        |
| 6.1.2.1.4. | Zuordnung von Verantwortlichkeiten und Aufgaben   | 59        |
| 6.1.2.1.5. | Einrichtung eines Überwachungssystems   | 59        |
| 6.1.2.1.6. | Dokumentation der getroffenen Maßnahmen   | 59        |
| 6.1.2.2.   | Unterschiede zum betriebswirtschaftlichen<br>Risikomanagement                           | 60        |
| 6.2.       | Internationale Anforderungen  | 63        |
| 6.2.1.     | COSO Internal Control – Integrated Framework  | 65        |
| 6.2.1.1.   | Aufbau und Ziele von COSO   | 65        |
| 6.2.1.2.   | Komponenten von COSO  | 66        |
| 6.2.1.2.1. | Control Environment (Steuerungsumfeld, Kontrollumfeld)                                  | 67        |
| 6.2.1.2.2. | Risk Assessment (Risikobeurteilung)   | 68        |
| 6.2.1.2.3. | Control Activities (Kontrollaktivitäten)  | 69        |
| 6.2.1.2.4. | Information & Communication (Information und<br>Kommunikation)                          | 69        |
| 6.2.1.2.5. | Monitoring (Überwachung)  | 70        |
| 6.2.1.3.   | Vergleich zum betriebswirtschaftlichen Risikomanagement                                 | 71        |
| 6.2.2.     | COSO - Enterprise Risk Management   | 73        |
| 6.2.2.1.   | Aufbau und Ziele von ERM  | 74        |
| 6.2.2.2.   | Komponenten von ERM   | 75        |
| 6.2.2.2.1. | Internal Environment (Internes Umfeld)  | 75        |
| 6.2.2.2.2. | Objective Setting (Zielbestimmung)  | 76        |
| 6.2.2.2.3. | Event Identification (Ereignisidentifikation)   | 77        |
| 6.2.2.2.4. | Risk Assessment (Risikobewertung)   | 77        |
| 6.2.2.2.5. | Risk Response (Risikosteuerung)   | 78        |
| 6.2.2.2.6. | Control Activities (Kontrollaktivitäten)  | 78        |
| 6.2.2.2.7. | Information and Communication (Information und<br>Kommunikation)                        | 78        |
| 6.2.2.2.8. | Monitoring (Überwachung)  | 79        |
| 6.2.2.3.   | Vergleich mit COSO I, IDW PS 340 sowie<br>dem betriebswirtschaftlichen Risikomanagement | 79        |
| <b>7.</b>  | <b>Zusammenfassung und Ausblick</b>   | <b>82</b> |
|            | <b>Literaturverzeichnis</b>   | <b>83</b> |
|            | <b>Literaturverzeichnis</b>   | <b>89</b> |
|            | <b>Autorenangaben</b>   | <b>94</b> |

## **Vorwort**

Die vorliegende Arbeit wurde im Wintersemester 2004/2005 am Fachbereich Wirtschaft der Hochschule Wismar als Diplomarbeit im Studiengang Betriebswirtschaft angenommen. Sie befasst sich mit einem im Rahmen der Corporate Governance-Diskussion hochaktuellen Thema, nämlich der Berücksichtigung nationaler und internationaler Prüfungsstandards im Rahmen des betrieblichen Risikomanagements.

Im Rahme des vorliegenden Bandes arbeitet die Verfasserin heraus, dass die Corporate Governance-Diskussion von unterschiedlichen Interessenlagen und Erwartungshaltungen geprägt ist. Aus Sicht betroffener Unternehmen besteht Interesse an einer redundanzfreien und integrierten Lösung, die die risiko- und chancenorientierte Unternehmenssteuerung gezielt unterstützt. Die Prüferseite hat gegebenenfalls ein Interesse an leichter prüfbareren aufgesetzten Lösungen, fokussiert eher Risiken als Chancen und sieht in Regelungen wie dem KonTraG oder dem Sarbanes-Oxley-Act auch eine Sicherung eigener Auftragsbestände. In diesem Spannungsfeld bezieht die Verfasserin sehr eigenständig und auf Basis einer fundierten Analyse Position.

Sie arbeitet aber auch heraus, dass im Zeitablauf eine Konvergenz von Anforderungen zu erwarten ist – dies gilt jedenfalls dann, wenn das im Herbst 2004 vorgelegte COSO II – Enterprise Risk Management international eine vergleichbar große Bedeutung für die Entwicklung internationaler Prüfstandards entwickelt wie der Vorläufer COSO I.

Die Verfasserin hat eine Arbeit vorgelegt, die für die Unternehmenspraxis ebenso wie für die Prüfungspraxis von großem Interesse ist. Ich freue mich, ihre Ausführungen im Rahmen dieser Schriftenreihe einem größeren Publikum zugänglich machen zu dürfen.

Wismar, Frühjahr 2005

Julia Neumann-Szyszka

## 1. Einleitung

Das Risikomanagement ist schon seit Jahrzehnten ein Thema der wissenschaftlichen Forschung und Praxis, und es existieren bereits zahlreiche betriebswirtschaftliche Konzeptionen und Methoden. Doch insbesondere in den letzten Jahren gewann das Risikomanagement zunehmend an Bedeutung, da die Unternehmen immer vielfältigeren und höheren Risiken ausgesetzt sind. Die Ursachen hierfür liegen in der fortschreitenden Globalisierung, in dem damit steigenden Wettbewerbsdruck, in dem raschen Technologiewandel sowie in immer komplizierter und unübersichtlicher werdenden Rahmenbedingungen (vgl. Seidel 2002: 23). Diese sich stetig veränderbaren Umfeldbedingungen und die daraus resultierenden Risiken machen die Einführung eines Risikomanagements unerlässlich, um den Fortbestand eines Unternehmens zu sichern (vgl. Maier 2001: 4). Dies spiegelt sich auch in den zahlreich gestiegenen Unternehmensschieflagen wider. In Deutschland sind beispielsweise die Bremer Vulkan AG oder die Metallgesellschaft AG (vgl. Kajüter 2003: 43) zu nennen. Diese Kapitalgesellschaften waren oft nicht in der Lage, Risiken frühzeitig zu erkennen und zu bewältigen. Nach Eintritt der Risiken waren Gegensteuerungsmaßnahmen bereits wirkungslos, so dass die Unternehmen in eine folgenschwere Krise gerieten. Diese hätte jedoch nicht selten durch die Implementierung eines effektiven Risikomanagements vermieden und in ihren negativen Folgen abgeschwächt werden können.

Dies hat auch der Gesetzgeber in Deutschland erkannt und im Jahre 1998 mit dem KonTraG eine gesetzliche Verpflichtung für Vorstände von Aktiengesellschaften zu einer angemessenen Risikofrüherkennung und –überwachung geschaffen. Des Weiteren geriet die Regierung zunehmend unter Handlungsdruck, weil Investoren und Kreditgeber verstärkt genauere Informationen und Kontrollen über die jeweilige Unternehmenspolitik und die mit ihr verbundenen Risiken erwarteten, da sie aufgrund der vielen Unternehmenskrisen ihr Vertrauen in Aufsichtsgremien und Abschlussprüfer verloren haben (vgl. Alquen 1999: 15). Um den Finanzplatz Deutschland wieder zu stärken, fordert der Gesetzgeber mit dem KonTraG auch eine Berichterstattung über die Risiken der künftigen Entwicklung der Unternehmen sowie eine Überprüfung durch den Abschlussprüfer, ob Maßnahmen zur frühzeitigen Erkennung von Risiken in den Unternehmen umgesetzt werden (vgl. Picot 2001: 18). Mit der Prüfungspflicht entwickelte sich das Risikomanagement auch vermehrt zu einem Thema der Wirtschaftsprüferpraxis, so dass das IDW einen Prüfungsstandard (IDW PS 340) geschaffen hat, der indirekt Mindestanforderungen (vgl. Vogler/Engelhard 2000: 1426) an ein im Unternehmen zu implementierendes Risikofrüherkennungs- und Überwachungssystem stellt.

Das KonTraG wiederum fand Ergänzung und Änderung durch weiterführende gesetzliche Reformen wie dem Transparenz- und Publizitätsgesetz

(TransPuG) im Juli 2002 und dem Bilanzrechtsreformgesetz (BilReG) im Dezember 2004.<sup>1</sup>

Doch nicht nur in Deutschland stand man diesen Problemen gegenüber, sondern auch international hat das Thema Risikomanagement große Aufmerksamkeit auf sich gezogen. So haben insbesondere in den USA in jüngster Vergangenheit spektakuläre Unternehmenskrisen (Enron, Worldcom) (vgl. Kauffmann/Götzenberger 2003: 151) zu öffentlichen Diskussionen geführt. Obwohl hier bereits seit 1992 mit COSO I (Internal Control – Integrated Framework) ein Verhaltenskodex existiert, der als Grundlage zur Identifikation, Bewertung, Kommunikation und Überwachung von Risiken weit reichende Akzeptanz erlangt hat (vgl. Kajüter 2003: 43) und die Basis für viele internationale Prüfungsstandards darstellt (z. B. ISA 315) (vgl. Menzies 2004: 86), kam es auch hier immer wieder aufgrund eines fehlenden Risikobewusstseins und eines mangelhaften Risikomanagements zu Krisen in Unternehmen. Dies führte schließlich zu einer Weiterentwicklung bzw. Ergänzung von COSO I zu COSO II, einem Enterprise Risk Management, das eine stärkere Risikoorientierung aufweist als COSO I und für alle Unternehmen unabhängig von Größe und Branche als Orientierungshilfe zur Implementierung eines Risikomanagements empfohlen wird. COSO II wurde am 29. September 2004 endgültig verabschiedet<sup>2</sup> und bestätigt die fortdauernde Aktualität des Themas „Risikomanagement“.

Das Ziel dieser Arbeit besteht darin, die betriebswirtschaftlichen Anforderungen an ein Risikomanagement darzustellen und mit den nationalen und internationalen (teilweise gesetzlichen) Anforderungen sowie Prüfungsstandards zu vergleichen. Dabei ist zu untersuchen, ob bereits mit der Einführung eines betriebswirtschaftlichen Risikomanagements im Unternehmen alle gesetzlichen Pflichten sowie Forderungen der Abschlussprüfer erfüllt sind oder ob Ergänzungen vorgenommen werden müssen.

Dafür ist es in einem ersten Schritt notwendig, den Begriff Risiko zu definieren, da dieser in der betriebswirtschaftlichen Literatur unterschiedliche Verwendung findet, aber gleichzeitig die Grundlage für das Verständnis der verschiedenen Risikomanagementkonzeptionen bildet. Nach der Begriffsklärung gilt es Risikoarten und Risikokategorien herauszustellen, denen die Unternehmen ausgesetzt sind. Sie unterstreichen noch einmal die Notwendigkeit zur Einführung eines Risikomanagementsystems, um den Fortbestand eines Unternehmens zu sichern. Dieses Ziel kann jedoch nur erreicht werden, wenn bestimmte betriebswirtschaftliche Anforderungen an ein Risikomanagement erfüllt werden, die im nächsten Schritt dargestellt werden sollen. Da ein betriebswirtschaftliches Risikomanagement sehr facettenreich und unternehmensindividuell auszugestalten ist, können hier nur konzeptionelle Grundla-

---

<sup>1</sup> [www.bmj.de/media/archive/649.pdf](http://www.bmj.de/media/archive/649.pdf), vom 4. Oktober 2004.

<sup>2</sup> [www.coso.org](http://www.coso.org), vom 30. September 2004.



gen erläutert werden.

Nach der Betrachtung aus betriebswirtschaftlicher Perspektive folgt im nächsten Abschnitt eine Darstellung der nationalen und internationalen Anforderungen an ein Risikomanagement. In Deutschland beziehen sich die Ausführungen vor allem auf die bereits erwähnten Gesetzesgrundlagen KonTraG, TransPuG, BilReG sowie auf den IDW PS 340.

Im internationalen Bereich beschränken sich die Ausführungen auf die Rahmenbedingungen in den USA, da COSO I eine Vorbildfunktion für viele nationale Regelwerke („Codes of Best Practise“) in anderen Ländern ausübt. In diesem Abschnitt gilt es insbesondere die Weiterentwicklung von COSO I zu COSO II zu untersuchen, um letztendlich beide COSO-Rahmenwerke den nationalen Gegebenheiten gegenüberstellen und mit den betriebswirtschaftlichen Anforderungen an ein Risikomanagement vergleichen zu können.

## 2. Risikobegriff

Bevor die grundlegenden Anforderungen an ein Risikomanagement dargestellt werden können, gilt es in diesem Abschnitt zu untersuchen, was unter dem Begriff „Risiko“ zu verstehen ist. Dabei ist zu beachten, dass hier keine allgemein gültige Definition angeführt werden kann. Selbst die Betriebswirtschaftslehre konnte sich noch auf kein einheitliches Begriffsverständnis einigen und auch für die **sprachliche Herkunft** sind in der Literatur unterschiedliche Erklärungsansätze zu finden.

So besagt eine etymologische<sup>3</sup> Herleitung von „Risiko“, dass das Wort vom lateinischen „resecum“ (= Felsklippe) stammt und sich im Laufe der Zeit aufgrund dessen, dass die Klippe insbesondere eine Gefahr für die Seefahrer darstellt, im Deutschen schließlich zu der Bedeutung „Gefahr“ oder „Wagnis“ (vgl. Sitt 2003: 2f) entwickelt hat.

Ein anderer Ansatz leitet „Risiko“ vom frühitalienischen „risicare“ ab, das „wagen“ im Sinne eines Abwägens oder einer Wahlentscheidung<sup>4</sup> bedeutet. Nach der Erläuterung der sprachlichen Herkunft von „Risiko“ soll nun die **inhaltliche Bedeutung** des Begriffs im Vordergrund stehen. Da das Begriffsverständnis in der Betriebswirtschaftslehre sehr unterschiedlich ist, sollen sich die Ausführungen auf eine weit verbreitete Sichtweise in der Literatur beschränken. Danach sind Risiken „...zukünftige Ereignisse und mögliche Entwicklungen innerhalb und außerhalb des Unternehmens, die zu einer (...) Verfehlung der Unternehmensziele führen können“ (Diederichs/Form/Reichmann 2004: 189). Bedingt wird dies durch eine **ursachenbezogene** und eine **wirkungsbezogene** Komponente (vgl. Kajüter 2003: 47).

<sup>3</sup> Ursprung und Geschichte der Wörter; Forschungsrichtung, die sich mit dem Ursprung der Geschichte der Wörter befasst.

<sup>4</sup> Vgl. Bernstein (1997: 18), zit. nach Kramer (2002: 157).

Die **ursachenbezogene** Komponente besagt, dass es aufgrund des Informationsdefizits des Entscheidungsträgers über die zukünftigen Entwicklungen und Ereignisse zu Verfehlungen der Unternehmensziele führen kann. Der Entscheidungsträger hat damit unvollkommene Informationen über künftige Umweltzustände und trifft seine unternehmerischen Entscheidungen unter Unsicherheit (vgl. Bitz 2000a: 235).

Demgegenüber stellt die **wirkungsbezogene** Komponente auf die mögliche Zielverfehlung und damit auf das Handlungsergebnis ab, so dass die Zielabweichung selbst als Risiko bezeichnet wird (vgl. Hölscher 2002: 5).

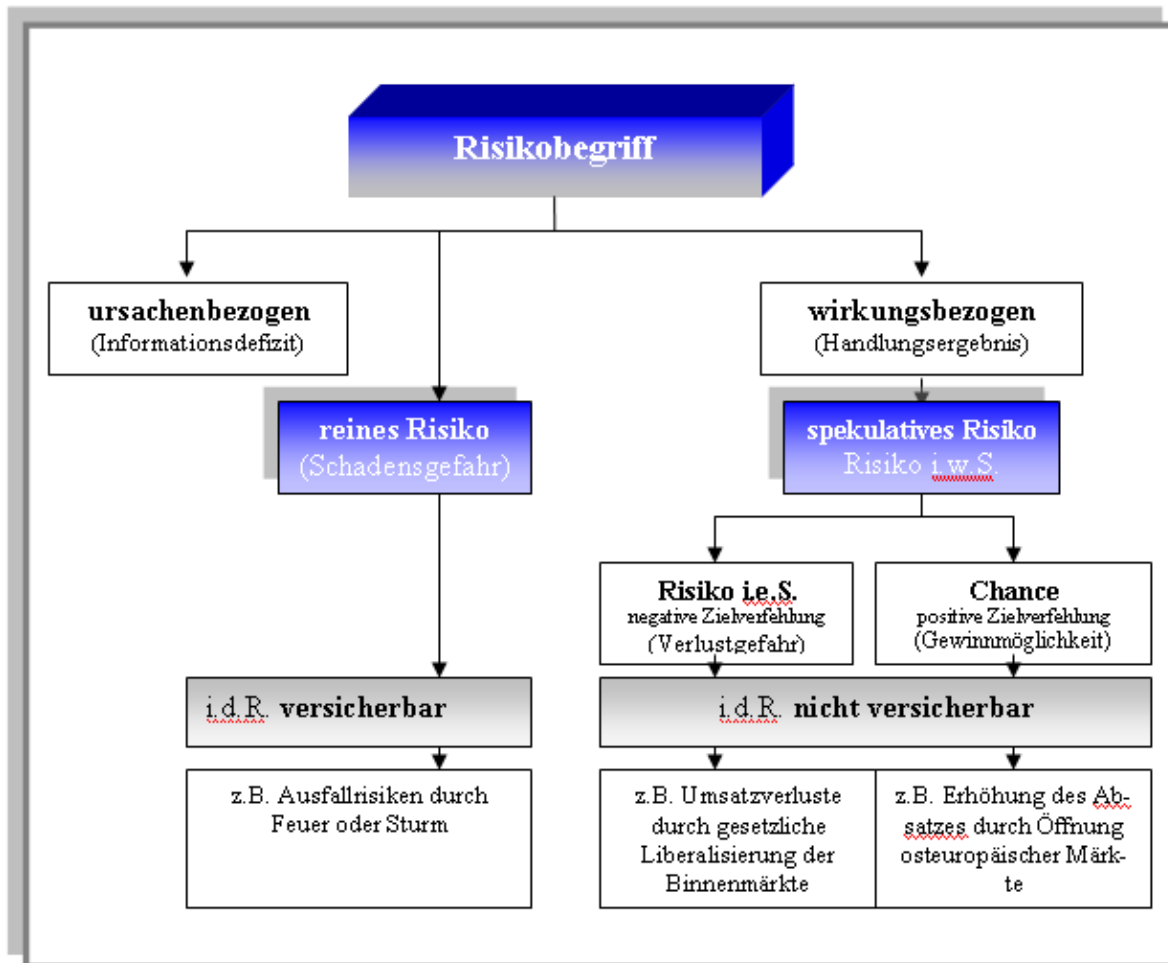
Handelt es sich bei der Zielverfehlung neben negativen Abweichungen auch um mögliche positive Abweichungen, d. h. Chancen, so ist auch von **spekulativen** Risiken bzw. Risiken i. w. S. die Rede. Diese spekulativen Risiken beziehen sich auf sämtliche unternehmerische Aktivitäten und Entscheidungen. Sie umfassen sowohl Verlustmöglichkeiten (= Risiken) als auch Gewinnmöglichkeiten (= Chancen) (vgl. Seidel 2002: 49).

Daneben existieren so genannte „**reine**“ **Risiken**, die nicht unmittelbar aus dem unternehmerischen Handeln heraus resultieren. Sie stellen vielmehr eine Schadensgefahr (z. B. Sturmschaden) dar, die selten und unregelmäßig in der Unternehmensentwicklung auftritt. Diese reinen Risiken zählen auch zu den so genannten **versicherbaren Risiken**, da Versicherungen die möglichen Schäden zum großen Teil abdecken können. Die spekulativen Risiken hingegen gehören zu den **nicht versicherbaren** Risiken (vgl. Hartmann 2003: 7). So ist z. B. das Risiko bei der Markteinführung eines neuen Produktes ein spekulatives (nicht versicherbares) Risiko, während das Risiko einer Flutkatastrophe ein reines (versicherbares) Risiko darstellt.

Die Abgrenzung zwischen spekulativen und reinen Risiken ist jedoch kritisch zu betrachten, weil eine eindeutige Differenzierung oft nicht möglich ist und gerade bei den spekulativen Risiken die Frage, welcher Teil einer Schwankungsbreite zur Verlustgefahr gehört und welcher zur Gewinnchance, vom Bezugspunkt abhängt (vgl. Liekweg 2003: 8f). Wie dieser Bezugspunkt zustande kommt, ist letztlich willkürlich und von der Risikoeinstellung des Entscheidungsträgers abhängig.

Die nachstehende Abbildung 1 soll die Zusammenhänge noch einmal verdeutlichen.

Abbildung 1: Systematik des Risikobegriffs



Quelle: In Anlehnung an Seidel (2002: 50).

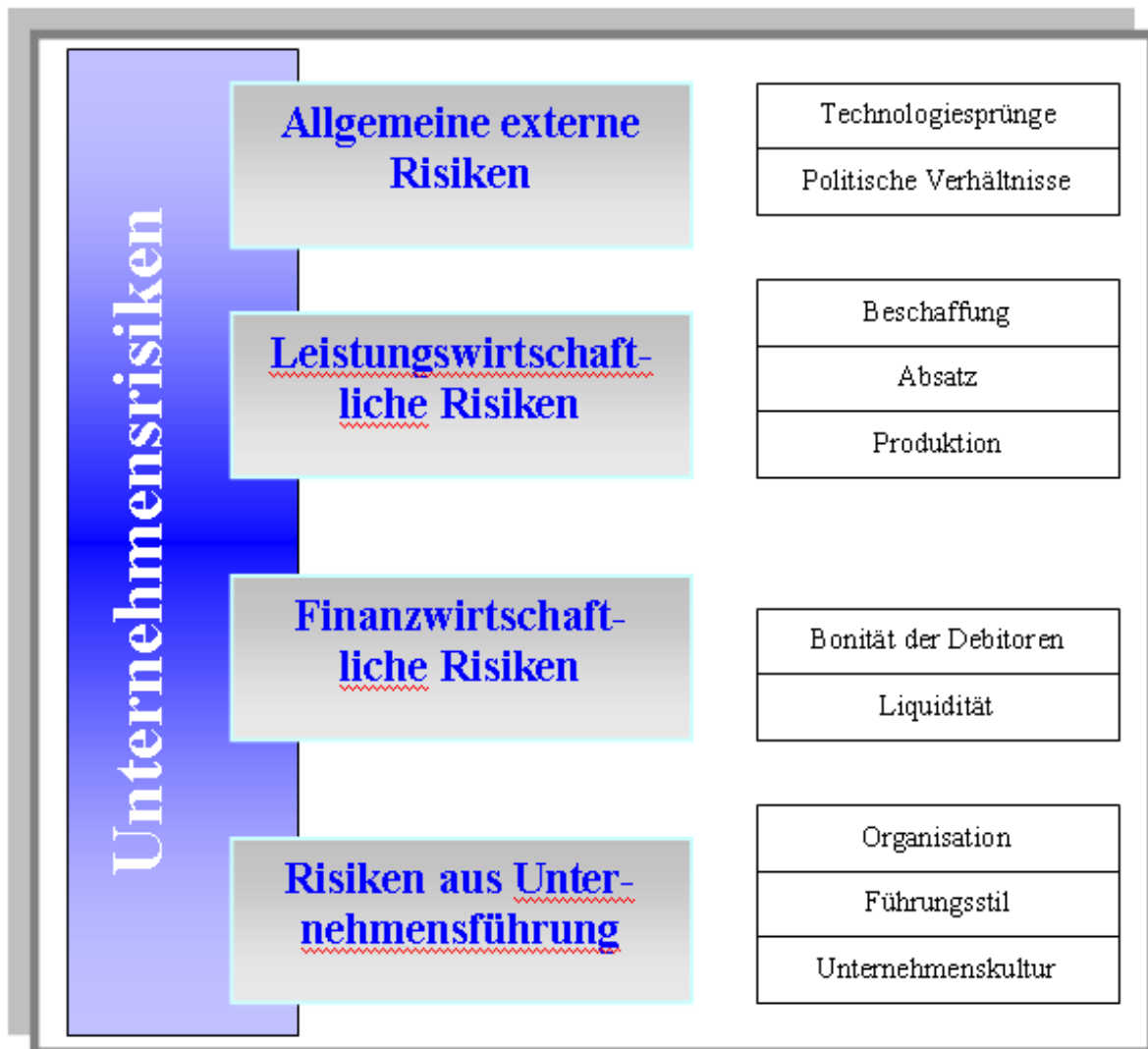
### 3. Risikoarten und -kategorisierung

Nachdem nun im Kapitel 2 der Risikobegriff erläutert wurde, besteht das Ziel dieses Abschnittes darin, grundlegende Risiken, denen die Unternehmen gegenüberstehen können, aufzuzeigen. Dies soll die Bedeutung und Notwendigkeit eines Risikomanagements im Unternehmen noch einmal hervorheben.

Grundsätzlich sind alle Unternehmen permanent sich wandelnden Rahmenbedingungen und daraus resultierenden vielfältigen Risiken ausgesetzt. Gesetzesänderungen, Währungsrisiken, demographische Veränderungen, Fertigungsrisiken, Konkurse wichtiger Kunden oder Systemausfälle sind nur einige Beispiele einer Vielzahl potenzieller Risiken. Da es aufgrund der Anzahl unmöglich wäre, alle Einzelrisiken aufzulisten und die Risikolandschaft eines Unternehmens je nach Branche und Marktstellung variiert (vgl. Burger/Buchhart 2002: 34ff), (so wird für einen Hersteller von PC-Prozessoren ein wesentlicher Risikoschwerpunkt in der Veränderung des technologischen

Umfeldes liegen; für ein Versorgungsunternehmen wird der Risikoschwerpunkt eher im Bereich der rechtlichen Rahmenbedingungen liegen), stellt die folgende Abbildung 2 eine Möglichkeit der Zusammenfassung der verschiedenen Risiken in Risikokategorien dar.

Abbildung 2: Risikokategorisierung



Quelle: Seidel (2002: 63).

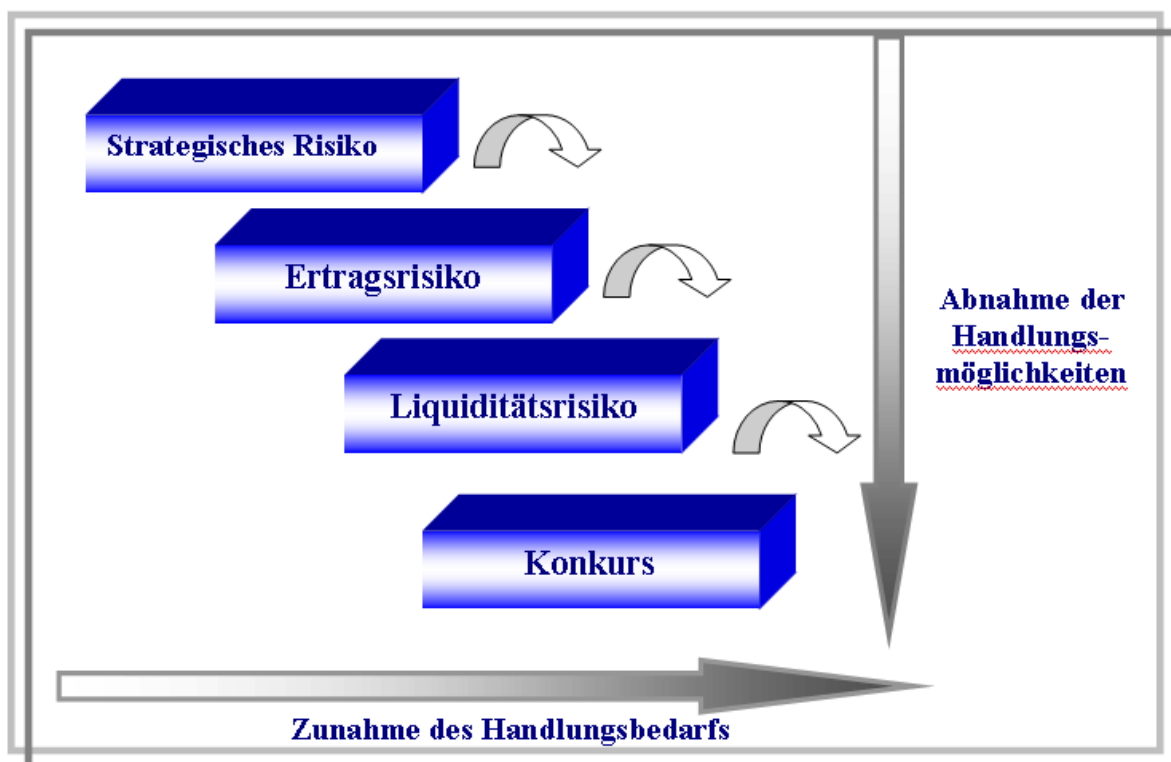
Von besonderer Bedeutung sind hier vor allem Risiken, die sich aus der Unternehmensführung ergeben. Das Management ist oft nicht in der Lage, Veränderungen im internen und externen Unternehmensumfeld frühzeitig wahrzunehmen (vgl. Lück 2000: 1473). Infolgedessen kann die Unternehmensstrategie nicht rechtzeitig an die veränderten Bedingungen angepasst werden. Die Ursache für die verspätete Wahrnehmung liegt darin begründet, dass in den meisten Unternehmen noch klassische Steuerungsinstrumente wie die Jahresabschlussanalyse zur Anwendung kommen (vgl. Seidel 2002: 20). Diese lösen

erst eine Warnfunktion aus, wenn bereits Umsatz- oder Ergebnisverschlechterungen eingetreten sind. In dieser Situation ist es meist nicht mehr möglich, wirkungsvolle Gegensteuerungsmaßnahmen einzuleiten. Das Unternehmen gerät in eine Erfolgskrise, die zwangsläufig zu Zahlungsschwierigkeiten führt. Häufig wird der Unternehmensleitung erst jetzt das Ausmaß der Krise bewusst, wenn die Insolvenz nicht mehr zu vermeiden ist (siehe Abbildung 3).

Schlussfolgernd lässt sich damit vor allem ein strategischer Fehler als der Beginn für eine spätere Unternehmenskrise beschreiben (vgl. Maier 2001: 9). Einige Literaturquellen gehen davon aus, dass über 60 % aller Unternehmensinsolvenzen auf derartige Managementfehler (vgl. Lück 2000: 1474) zurückzuführen sind.

Der Weg in die Insolvenz wird durch die Abbildung 3 noch einmal grafisch veranschaulicht.

Abbildung 3: *Entwicklung des Risikos*



Quelle: In Anlehnung an Kirchner (2002: 17).

Vor diesem Hintergrund ist die Implementierung eines Risikomanagements unerlässlich. Durch eine rechtzeitige Identifikation von Risiken mit Hilfe von Frühwarnindikatoren soll die Unternehmensleitung genügend Zeit gewinnen, um Krisen vom Unternehmen abzuwenden.

Die bis jetzt einseitige Darstellung der Risiken darf nicht zu der Ansicht führen, dass unternehmerisches Handeln darin besteht, sämtliche Risiken zu vermeiden. Unternehmen müssen sich auf die Erfolgsfaktoren stützen und ihre

unternehmerischen Chancen nutzen. Mit jeder Chance ist jedoch auch ein Risiko verbunden, so dass es langfristigen unternehmerischen Erfolg ohne Risiko nicht geben kann (vgl. Lück 2000: 1473). Schließlich bieten sich aus der Öffnung neuer Märkte zusätzliche Absatzchancen für Unternehmen, gleichzeitig geht damit aber auch eine Erhöhung des Wettbewerbs einher. Auch im Rahmen der technologischen Entwicklungen ergeben sich für Unternehmen Chancen und Risiken. So erleichtern sie für das Unternehmen den weltweiten Informationsaustausch, entsprechend vergrößert sich jedoch auch die Markttransparenz, was zu einem erhöhten Preisdruck führt.

Eine erfolgreiche Unternehmensführung besteht damit in der frühzeitigen Wahrnehmung von Chancen bei einer gleichzeitigen Verringerung von Risiken (vgl. Gleißner 2000: 1629). So kann selbst das Nichterkennen von Chancen ein erhebliches Risiko für das Unternehmen darstellen, weil auf Ertragsmöglichkeiten und Wettbewerbsvorteile verzichtet wird (vgl. Neubeck 2003: 23). Wichtig ist: Je höher das Risiko einer Strategie ist, desto höher sollten auch die Gewinnchancen sein (vgl. Brühwiler 2001: 7). Für eine Chancen- und Risikooptimierung stellt die Einführung eines Risikomanagements im Unternehmen – ebenso wie für die Risikosteuerung – eine Notwendigkeit dar.

#### 4. Begriff und Ziele des Risikomanagements

Da im Kapitel 3 die Bedeutung eines Risikomanagements für Unternehmen herausgestellt wurde, soll in diesem Abschnitt kurz auf die Entstehungsgeschichte des Begriffs eingegangen werden. Danach gilt es die wichtigsten Ziele aufzuzeigen, die aus heutiger Sicht mit einem Risikomanagement verbunden werden.

##### 4.1. Entstehung des Begriffs „Risikomanagement“

Der Begriff „Risikomanagement“ entstammt weniger einer wissenschaftlichen oder theoretischen Konzeption als vielmehr der amerikanischen Unternehmenspraxis (vgl. Liekweg 2003: 4). Über diese hat er schließlich auch im deutschsprachigen Raum Verbreitung gefunden.

In den sechziger Jahren betrieben insbesondere amerikanische Großunternehmen „Risk Management“, wobei die versicherbaren Risiken (= reine Risiken) im Mittelpunkt der Betrachtung standen und Risikomanagement mit **Versicherungsmanagement** gleichgesetzt wurde (vgl. Beinert 2003: 25). Damit bestand das Ziel darin, viele Risiken auf Versicherungen zu überwälzen. Immer höher steigende Versicherungsprämien führten jedoch dazu, dass die Unternehmen Risiken vermehrt selbst getragen haben (vgl. Hartmann 2003: 18) und ein systematischer Umgang mit Risiken erforderlich wurde. In westeuropäischen Unternehmen wurden daraufhin Abteilungen gegründet, die sich ausschließlich mit dem Managen von Risiken befassten (vgl. Neubeck 2003: 24). Es setzte sich die Erkenntnis durch, dass sich das systematische

Es setzte sich die Erkenntnis durch, dass sich das systematische Vorgehen des Risikomanagements auch auf andere Risiken erweitern lässt. Dies führte schließlich zu einer entsprechenden Erweiterung des Aufgabengebietes. Neben den versicherungstechnischen „reinen“ Risiken wurden nun auch zunehmend die Gewinn- und Verlustrisiken („spekulative“ Risiken) in die Untersuchungen einbezogen (vgl. Liekweg 2003: 4f). Zusätzlich veränderte sich der zeitliche Betrachtungsrahmen. Wurde anfangs lediglich versucht, auf bereits eingetretene Risikosituationen einzuwirken, so versuchte man nun Möglichkeiten zu finden, Risiken möglichst frühzeitig zu erkennen, um diesen rechtzeitig entgegenwirken zu können (vgl. Hartmann 2003: 19).

Daraus ergibt sich aus heutiger betriebswirtschaftlicher Sicht folgende Definition des Risikomanagements:

„Die Gesamtheit aller organisatorischen Regelungen und Maßnahmen zur Risikoerkennung und zum Umgang mit den Risiken aus unternehmerischer Betätigung werden als Risikomanagement bezeichnet“ (Diederichs/Form/Reichmann 2004: 189).

#### 4.2. *Ziele des Risikomanagements*

Oberstes Ziel des Risikomanagements ist es, die Unternehmensführung bei der **Sicherung des Unternehmensfortbestandes** zu unterstützen und damit die Unternehmensinsolvenz zu vermeiden. Das Risikomanagement fördert dabei einen bewussten und effizienten Umgang mit Risiken, so dass keine existenzgefährdende Situation entstehen kann. Dabei ist sicherzustellen, dass die Gesamtheit aller vorhandenen Risiken nicht die Risikotragfähigkeit (vgl. Kirchner 2002: 18) des Unternehmens übersteigt. Das Risikotragfähigkeitspotenzial eines Unternehmens ist dann überschritten, wenn bei gleichzeitigem Eintritt aller Risiken über die Hälfte des vorhandenen Eigenkapitals aufgezehrt wird (vgl. Diederichs/Form/Reichmann 2004: 193).

Über die Existenzsicherung hinaus zielt das Risikomanagement auch auf eine **Steigerung des Unternehmenswertes** ab. Denn durch das bewusste und kontrollierte Eingehen von Risiken können mit den damit einhergehenden Chancen höhere Wertbeiträge für das Unternehmen erzielt werden. Daraus ergibt sich, wie bereits erwähnt, dass nicht das Ziel der Risikovermeidung verfolgt werden darf, sondern vielmehr muss die Risikooptimierung und Chancennutzung im Vordergrund stehen. Mit dem Risikomanagement sollte also auch immer ein Chancenmanagement einhergehen (vgl. Kirchner 2003: 15). Langfristig wird das Unternehmen am erfolgreichsten sein, das seine Chancen am besten kennt und nutzt und das zugleich seine Risiken am besten kontrolliert und bewältigt.

Aus diesen Primärzielen ergeben sich weitere Unterziele für die Unternehmen, die beispielsweise in einer Steigerung des Marktanteils und in einer Erhöhung des Gewinns liegen können.

## 5. Betriebswirtschaftliche Anforderungen an ein Risikomanagementsystem

Um die zuvor genannten Ziele zu erreichen, ist es Aufgabe des Risikomanagements, risikobehaftete Entwicklungen und zukünftige Chancen frühzeitig zu identifizieren, zu analysieren, zu bewerten, zu kommunizieren, zu steuern und fortlaufend zu überwachen und damit das Unternehmen an die Dynamik der Umfeldbedingungen anzupassen. Welche Anforderungen sich daraus an ein Risikomanagement im Einzelnen ergeben, wird im folgenden Abschnitt untersucht. Es sei darauf hingewiesen, dass die Ausgestaltung eines Risikomanagements von der Größe, der Branche, der Struktur und Komplexität eines Unternehmens abhängig ist. Infolgedessen können in diesem Kapitel nur die grundlegenden konzeptionellen Anforderungen dargestellt werden und nicht deren konkrete Ausgestaltung.

### 5.1. Risikomanagementprozess

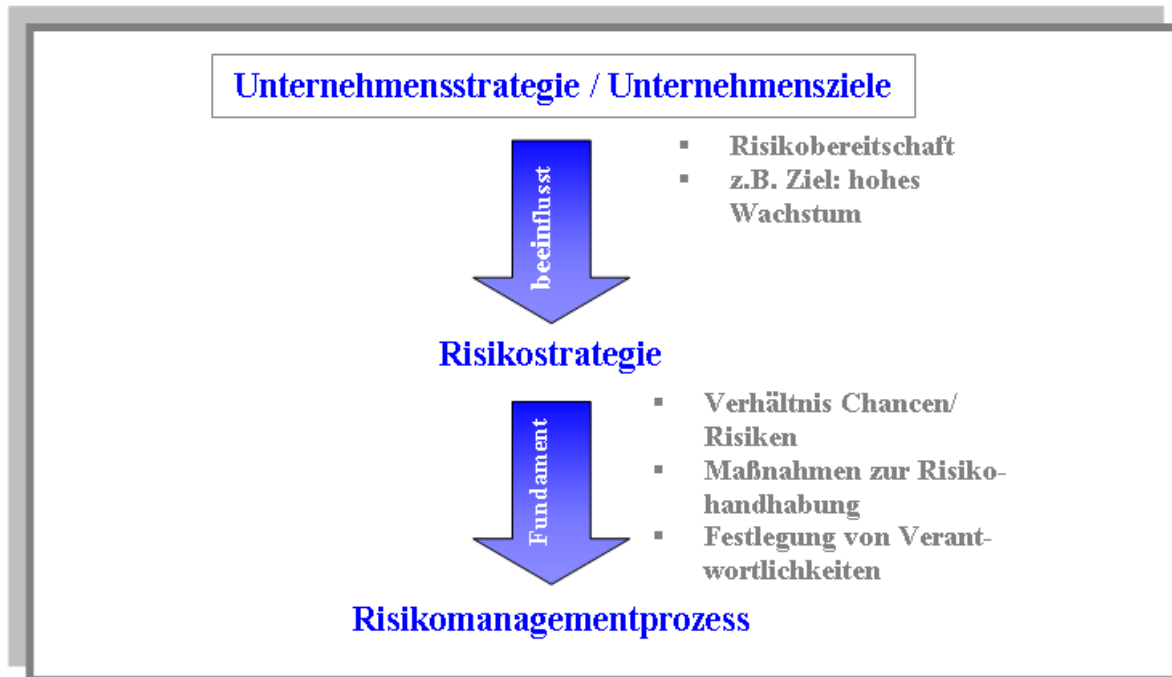
Risikomanagement läuft im Unternehmen als Prozess ab (vgl. Alquen 1999: 25). Obwohl dieser Prozess in der Literatur nicht einheitlich beschrieben wird und zahlreiche Unterschiede bei den einzelnen Prozessschritten sowie in deren Abgrenzungen bestehen, ergeben sich im Kern einheitliche Grundzüge und Anforderungen an ein Risikomanagementsystem, die nun im weiteren Verlauf vorgestellt werden sollen.

#### 5.1.1. Festlegung der Risikostrategie

Bevor das Risikomanagement als kontinuierlicher Prozess in einem Unternehmen eingeführt werden kann, muss zunächst eine Risikostrategie (vgl. Diederichs/Form/Reichmann 2004: 191) festgelegt werden. Diese soll das Risikobewusstsein im Unternehmen fördern (vgl. Reichmann/Form 2003: 169), so dass alle Mitarbeiter Risiken frühzeitig wahrnehmen und ihr unternehmerisches Handeln risikobewusst ausrichten. Des Weiteren dient die Risikostrategie als Fundament des gesamten Risikomanagementprozesses (siehe Abbildung 4) (vgl. Maier 2001: 4).



Abbildung 4: Strategische Ebene des Risikomanagements



Quelle: In Anlehnung an Gleißner (2000: 1628).

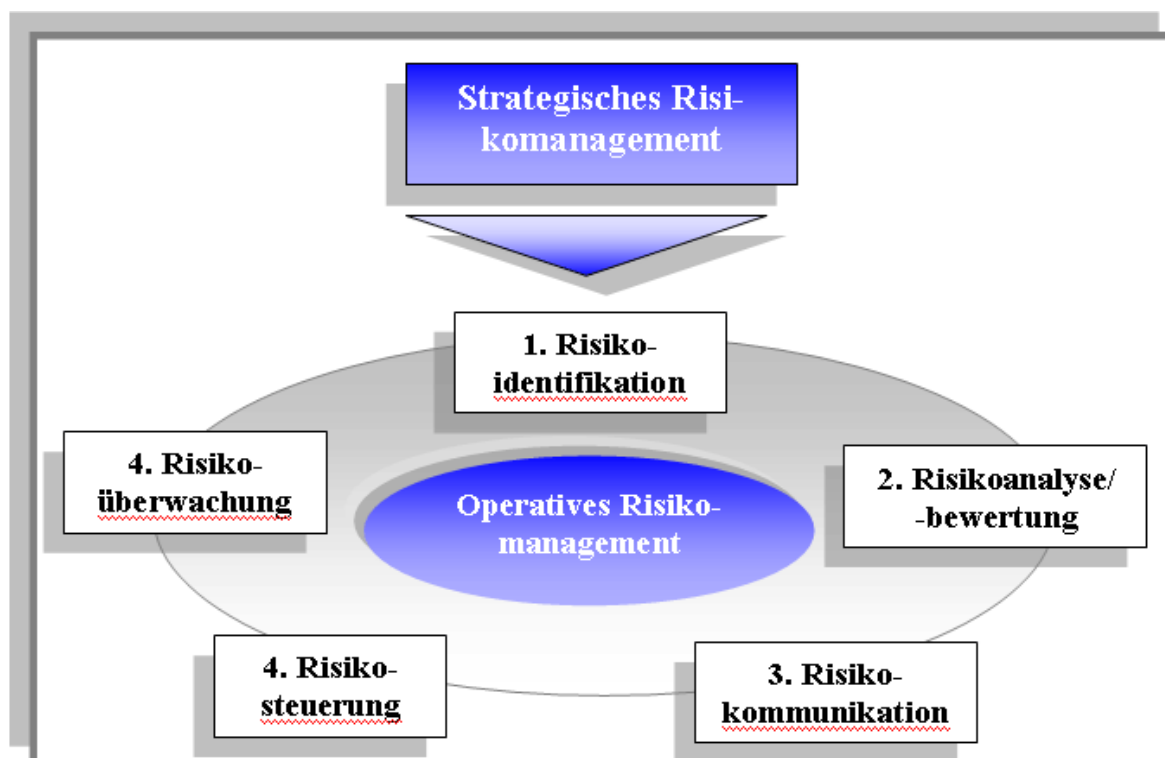
Sie beinhaltet vor allem die Formulierung von Risikomanagement-Zielen und die Festlegung, in welchem Verhältnis Chancen und Risiken zueinander stehen sollen (vgl. Gleißner 2000: 1627). Außerdem bestimmt sie Schwellenwerte für Risiken, ab denen Gegensteuerungsmaßnahmen getroffen werden müssen (vgl. Weber/Weißenberger/Liekweg 1999: 17). Zudem regelt sie die Verantwortlichkeiten für alle Risiken. Mit Hilfe dieser Richtlinien wird die Basis für eine Risikokultur und ein einheitliches Risikoverständnis im Unternehmen geschaffen (vgl. Diederichs/Form/Reichmann 2004: 191). Wichtig ist, dass die Risikostrategie nicht nur von der Unternehmensleitung vorgegeben, sondern auch von ihr „vorgelebt“ wird (vgl. Hohnhorst 2002: 98). Nur so wird sie auch von allen Mitarbeitern im Unternehmen akzeptiert. Grundsätzlich gibt es für die Risikostrategie keine allgemeingültigen inhaltlichen Vorgaben. Sie ist stets unternehmensspezifisch auszugestalten. Dabei hat sie sich an der jeweiligen Unternehmensstrategie und den Unternehmenszielen sowie an der Risikobereitschaft des Unternehmens (vgl. Gleißner 2000: 1628) auszurichten. Zwischen der festzulegenden Risikostrategie und der Unternehmensstrategie besteht damit eine Wechselwirkung. So ist eine Unternehmensstrategie, die auf ein hohes Wachstum abzielt, in der Regel mit hohen Risiken verbunden.

Letztendlich soll die Risikostrategie die Unternehmensführung bei der Erreichung der Unternehmensziele unterstützen. Risikomanagement ist damit als risiko- und chancenbewusste Unternehmensführung zu verstehen. Dies hat zur Konsequenz, dass Risikomanagement nicht separat abläuft, sondern vielmehr

einen integrativen Bestandteil (vgl. Weber/Weißenberger/Liekweg 1999: 11) im System „Unternehmen“ darstellt. Daher stammt auch der Begriff **Risikomanagementsystem**, weil es als Subsystem in einem offenen, komplexen, dynamischen und sozialen System (Unternehmen) aus verschiedenen Elementen (z. B. Regeln, Maßnahmen, Prozessen) besteht, die miteinander in wechselseitiger Beziehung stehen (vgl. Neubeck 2003: 2). Durch die Integration des Risikomanagements in das Unternehmen sollen insbesondere vorhandene Strukturen genutzt werden, so dass auf den Aufbau einer eigenständigen Organisationsstruktur für das Risikomanagement verzichtet werden kann und sich damit Kostenvorteile (vgl. Weber/Weißenberger/Liekweg 1999: 11) ergeben. Außerdem ermöglicht die Integration die Einbindung des Risikomanagements in bereits vorhandene Planungen, die ebenfalls Chancen und Risiken beinhalten, so dass Redundanzen verhindert werden können. Hinzu kommt, dass es ein Risikobewusstsein bei allen Unternehmensangehörigen fördert, weil alle Mitarbeiter in das Risikomanagement mit eingebunden werden.

Nach der Festlegung der Risikostrategie ergibt sich für den Risikomanagementprozess nun folgender Ablauf:

*Abbildung 5: Risikomanagementprozess auf der operativen Ebene*



Quelle: In Anlehnung an [www.risknews.de](http://www.risknews.de), 27.06.2004.

Prinzipiell bauen die einzelnen Phasen des Prozesses (siehe Abbildung 5) aufeinander auf und bilden einen Kreislauf. So setzt eine Bewertung von Risiken z. B. voraus, dass vorab eine Identifikation der zu bewertenden Risiken statt-

gefunden hat. Die Einleitung einer Steuerungsmaßnahme ist wiederum abhängig vom Ergebnis der Risikobewertung, welches dem zuständigen Entscheidungsträger kommuniziert wird. Dies bedeutet jedoch nicht, dass der Prozess als zwangsläufig sequentielle Abfolge stattfinden muss. Es kann jederzeit auch auf vor- oder nachgelagerte Prozessschritte gesprungen werden. Jedoch ermöglicht die bewusste Einführung eines Prozesses erst eine Systematik und eine Wiederholung (vgl. Kirchner 2002: 15). Insbesondere der Wiederholung kommt eine große Bedeutung zu, da sich durch die Komplexität und Dynamik der Umwelt die Risikostrukturen des Unternehmens und die sich bietenden Chancen fortlaufend ändern (vgl. Weber/Weißberger/Liekweg 1999: 16).

### 5.1.2. Risikoidentifikation

Ein effektives Risikomanagement ist nur möglich, wenn detaillierte Kenntnisse über sämtliche Risiken aus allen Bereichen des Unternehmens vorhanden sind. Die Identifikation der Risiken bildet vor allem auch eine wichtige Informationsgrundlage für die nachfolgenden Prozessschritte der Risikobewertung und -steuerung. Denn nur diejenigen Risiken können bewertet und gesteuert werden, die zuvor auch identifiziert wurden (vgl. Seidel 2002: 62). Damit wird die Effektivität des Risikomanagements bereits in diesem Prozessschritt bestimmt (vgl. Wolf 2004: 214). Eine Beschränkung auf bereits vorher definierte Risiken darf nicht erfolgen, da ansonsten die Objektivität der Risikoidentifikation zu stark eingeschränkt wird (vgl. Neubeck 2003: 73).

Das Ziel der Risikoidentifizierung besteht damit in einer **unternehmens-einheitlichen, systematischen, wirtschaftlichen, frühzeitigen und permanenten** Erfassung **bestehender, potenzieller und latenter Risiken** des Unternehmens.

Um dies zu ermöglichen, ist es zweckmäßig, vorher Risikofelder und damit eine Risikokategorisierung festzulegen, da dadurch der Einsatz von geeigneten Methoden zur Identifikation von Risiken erleichtert wird (vgl. Reichmann/Form 2003: 169). Die Vielfalt der Risiken macht es jedoch schwierig eine klare Strukturierung vorzunehmen, so dass es sich aber grundsätzlich anbietet eine Klassifizierung wie sie im Kapitel 3 dargestellt wurde, vorzunehmen. Da die Risikoidentifikation aus Sicht des gesamten **Unternehmens** und **einheitlich** erfolgen soll, muss in einem Top-down-Ansatz, d. h. ausgehend von der Unternehmensleitung, diese grobe Risikokategorisierung vorgegeben und dann im Wege eines Bottom-up-Ansatzes durch die operativen Einheiten im Unternehmen konkretisiert werden. Es handelt sich somit um einen kombinierten Top-down- und Bottom-up-Ansatz (vgl. Seidel 2002: 62). Grundsätzlich ist die Risikoidentifikation damit Aufgabe der operativen Geschäftsbereiche, da die Mitarbeiter vor Ort am besten wissen, welche Risiken in ihrem Tätigkeitsfeld auftreten können (vgl. Vogler/Grundert 1998: 2380).

Um den Anforderungen der **systematischen** Risikoerfassung (vgl. Bre-

beck/Herrmann 1997: 384) zu genügen, bieten sich beispielsweise folgende Identifikationsmethoden<sup>5</sup> an:

- Checklisten
- schriftliche Befragung
- Interview
- SWOT-Analyse (Stärken-Schwächen-Analyse)
- Brainstorming
- **PEST-Konzept**
- **Wertschöpfungskette nach Porter**
- Workshops
- Bilanzanalyse
- Szenarioanalysen

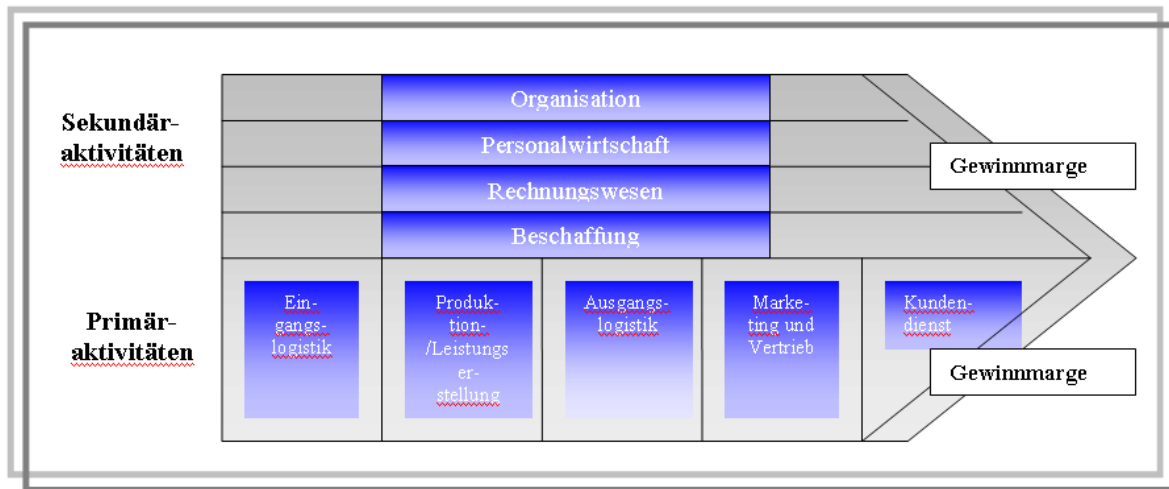
Ausgehend von der Risikokategorisierung in Kapitel 3 kann zur Identifikation der **allgemeinen externen Risiken** das **PEST-Konzept** (Political, Economic, Social, Technological) zur Anwendung kommen. Dieses gibt eine Systematik zur Identifikation der Risiken in der Makroumwelt vor. Hierbei geht es um eine Analyse ökonomischer, politisch/rechtlicher, sozialer und technologischer Umweltrisiken. Informationen und Daten über die allgemeine Entwicklung der Makroumwelt können von Ministerien, Forschungsinstituten, von Verbänden oder aus Datenbanken gewonnen werden. Da nicht alle Entwicklungen in der Makroumwelt für das einzelne Unternehmen relevant sind, müssen die meist allgemein gehaltenen Daten für die speziellen Informationszwecke des Unternehmens aufbereitet werden (vgl. Martin/Bär 2002: 94).

Zur Identifikation der **leistungswirtschaftlichen**, der **finanzwirtschaftlichen** und der **Risiken aus der Unternehmensführung** bietet beispielsweise eine Orientierung an der **Wertschöpfungskette nach Porter** (siehe Abbildung 6) ein systematisches Vorgehen (vgl. Dahms 2003: 219).

---

<sup>5</sup> Vgl. Zellmer (1990: 32ff); u. a. Martin/Bär (2002: 92).

Abbildung 6: Wertschöpfungskette nach Porter



Quelle: In Anlehnung an Weber/Weißenberger/Liekweg (1999: 14).

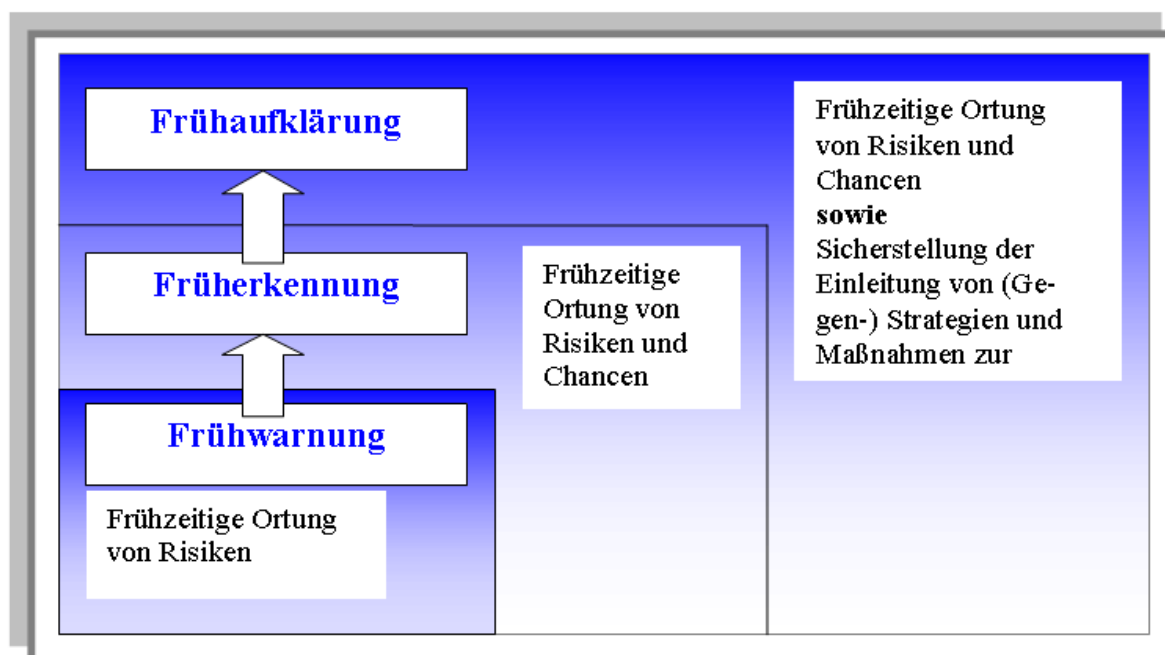
Damit finden die Risiken, die sich aus den primären Unternehmensaktivitäten wie Logistik, Produktion und Absatz ergeben, Berücksichtigung. Auch die Risiken aus den Sekundäraktivitäten, welche die Primäraktivitäten unterstützen, werden hiermit erfasst. Die Sekundäraktivitäten entsprechen dabei der Unternehmensführung, der Organisation, der Personalwirtschaft, dem Rechnungswesen und der Beschaffung.

Bei der Auswahl der jeweiligen Identifikationsmethode ist besonders das Wirtschaftlichkeitsprinzip (vgl. Brebeck/Herrmann 1997: 384) zu beachten. So ist z. B. eine schriftliche Befragung der Mitarbeiter sehr aufwendig und kann unter Umständen nicht zu den gewünschten Ergebnissen führen. Zusätzlich hängt die Wahl der Methodik von den spezifischen Risikoprofilen des Unternehmens und der Branche ab. In der betrieblichen Praxis findet häufig auch eine Kombination einzelner Identifikationsmethoden statt. Doch unabhängig für welche Methode sich die einzelnen Unternehmensbereiche entscheiden, besteht ein wesentliches Problem darin, dass keine Methode die vollständige Erfassung aller Risiken garantieren kann (vgl. Kindler/Pahlke 2001: 69f).

Bei der Risikoidentifikation gilt es vor allem zu bedenken, dass die einmal erkannten Risiken nicht konstant bleiben bzw. sich zwingend kontinuierlich entwickeln. Daher ist die Aufgabe der Risikoidentifikation **permanenter** Natur, um diese Veränderungen **rechtzeitig** wahrnehmen zu können (vgl. Romeike 2003b: 165).

Weiterhin muss berücksichtigt werden, dass insbesondere bei neu auftretenden Risiken für das Unternehmen die Schwierigkeit in einer **frühzeitigen** Identifikation und Erfassung besteht, so dass die Implementierung eines **Frühwarnsystems** notwendig ist (vgl. Seidel 2002: 48). Solch ein Frühwarnsystem ermöglicht eine rechtzeitige Identifikation von Risiken, um noch hinreichend Zeit für die Ergreifung geeigneter Gegenmaßnahmen zu haben.

Abbildung 7: Frühaufklärung, Früherkennung, Frühwarnung



Quelle: Horvath (2003b: 217).

Entscheidend hierfür ist die Suche nach Frühwarnindikatoren (z. B. Konjunkturindizes, Fluktuation des Personals) qualitativer und quantitativer Art, die sich mit zeitlichem Vorlauf zu dem identifizierten Risiko verändern und somit Signalwirkung haben (vgl. Neubeck 2003: 77). Frühwarnsysteme verschaffen Zeit für Reaktionen und verbessern damit die Steuerbarkeit eines Unternehmens. Sie stellen die wichtigsten Instrumente zur Risikoidentifikation dar (vgl. Lück 2000: 1476). Eine Weiterentwicklung der Frühwarnsysteme sind so genannte **Früherkennungssysteme** (vgl. Krystek 1999: 147). Diese unterscheiden sich im Wesentlichen von erst genannten Systemen dadurch, dass nicht nur Risiken als negative Zielverfehlung, sondern auch positive Zielverfehlungen, also Chancen betrachtet werden. Wird zusätzlich noch der Prozessschritt der Risikosteuerung und -kontrolle berücksichtigt, so wird der Begriff **Frühaufklärung** (vgl. Krystek 1999: 147) verwendet (siehe Abbildung 7), wobei diese Phasen des Risikomanagementprozesses erst in den kommenden Abschnitten im Mittelpunkt stehen.

Die betriebswirtschaftliche Forschung fordert vor allem die Anwendung von Frühaufklärungssystemen, in denen Chancen ebenso betrachtet werden wie Risiken. Die Identifizierung von Chancen erfolgt damit parallel zur Risikoidentifikation. Hier haben sich in der Praxis Methoden wie **Workshops** (Brainstorming) oder Interviews bewährt. Man erkennt damit zunehmend auch in der Praxis den Vorteil eines Chancenmanagements (vgl. Helmke/Risse 1999: 279).

Zum Abschluss der Risikoidentifikation wird ein **Risikoinventar** (siehe

Anhang 1) erstellt. Dieses beinhaltet die Auflistung aller identifizierten Risiken. Mehrfachnennungen können somit entdeckt und eliminiert werden. Im Risikoinventar werden zudem ähnliche Risiken gruppiert, um einen systematischeren Einblick zu erhalten und damit die weiteren im Risikomanagementprozess folgenden Teilprozesse zu beschleunigen (vgl. Neubeck 2003: 76). Unmittelbar an die Risikoidentifikation schließt sich nun die Risikobewertung an.

### 5.1.3. Risikoanalyse und -bewertung

Den Ausgangspunkt für diese Phase des Risikomanagementprozesses bildet das Risikoinventar (vgl. Neubeck 2003: 79). Die im Risikoinventar aufgelisteten Risiken werden zunächst **analysiert**. Dabei ist für jedes Risiko der jeweilige Ursprung zu bestimmen. Dies ist für die Feststellung wichtig, ob die Ursache für das Risiko inner- oder außerhalb des Unternehmenseinflussbereiches liegt (vgl. Lück 2000: 1476).

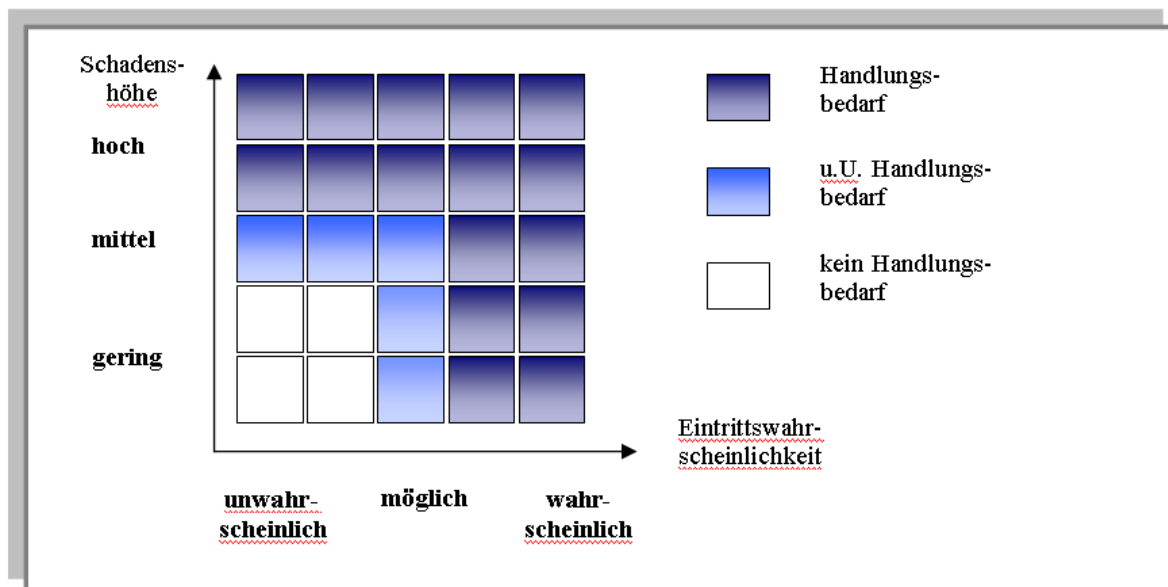
Im Anschluss an die Risikoanalyse erfolgt eine **quantitative Bewertung** oder **qualitative Beurteilung** der identifizierten Risiken. Eine Bewertung und Beurteilung ist notwendig, um Risiken entsprechend ihrer Bedeutung für das Unternehmen zu klassifizieren (gering, mittel, hoch, bestandsgefährdend) (vgl. Kajüter 2003: 55) und um mit Hilfe dieser Bewertungsgrundlage Kosten und Nutzen für eventuelle Gegensteuerungsmaßnahmen gegenüberstellen zu können. Bei der **quantitativen Bewertung** wird ein Schadenerwartungswert ermittelt, der sich aus der Multiplikation der beiden Kriterien Eintrittswahrscheinlichkeit und Schadenshöhe eines einzelnen Risikos ergibt (Brutto-Risikowert) (vgl. Romeike 2003a: 179). Werden bereits ergriffene Gegenmaßnahmen in die Risikoquantifizierung mit einbezogen, so gelangt man zum Netto-Risikowert (Schadenerwartungswert abzüglich der Kosten für die Gegenmaßnahmen) (vgl. Diederichs/Form/Reichmann 2004: 193).

Kritisch ist dabei anzumerken, dass diejenigen Risiken mit geringer Eintrittswahrscheinlichkeit, aber einem hohen drohenden Schaden genauso bewertet werden wie Risiken mit einem geringeren Vermögensverlust und einer hohen Eintrittswahrscheinlichkeit. Obwohl beide Arten von Risiken einen identischen Schadenerwartungswert aufweisen können, bedürfen sie jedoch im Regelfall einer unterschiedlichen Handhabung. Priorität sollte nach Wolf/Runzheimer dabei aber immer auf das Risiko mit der hohen Schadenshöhe gelegt werden, da dies eine größere Bedrohung für das Unternehmen darstellt (vgl. Wolf/Runzheimer 2003: 66).

Für die weiteren Steuerungsmaßnahmen bietet es sich an, die Ergebnisse der Risikoquantifizierung in einem Koordinatensystem zu visualisieren, dessen Ordinate die Schadenshöhe und dessen Abszisse die Eintrittswahrscheinlichkeit abbildet. Dieses Koordinatensystem wird in der Literatur auch als **Risikoportfolio** oder **Risikomatrix** (vgl. Hölscher 2002: 9) bezeichnet. Hierbei

handelt es sich um ein Portfolio, in dem die **Einzelrisiken** einer organisatorischen Einheit (z. B. Geschäftsbereich) dargestellt werden können (vgl. Kajüter 2003: 55). Risiken werden hier gemäß ihrer Gefährdungspotenziale für das Unternehmen in eine Rangordnung gebracht. Mit Hilfe dieses Portfolios können in der Folge Normstrategien zur Handhabung der verschiedenen Risiken abgeleitet (vgl. Wolf/Runzheimer 2003: 137) und damit Sollvorgaben vorgegeben werden (siehe Abbildung 8).

Abbildung 8: Risikomatrix



Quelle: In Anlehnung an Wolf/Runzheimer (2003: 137).

Je weiter ein Risiko in der oberen rechten Ecke des Portfolios liegt, desto größer ist seine Dringlichkeit und desto mehr wird das Unternehmen durch den Risikoeintritt geschädigt.

In analoger Weise können auch die identifizierten Chancen quantifiziert und in einer so genannten „Chancenmatrix“ dargestellt werden.

Ein erheblicher Nachteil der Verwendung der Risikomatrix besteht darin, dass keine Interdependenzen zwischen verschiedenen Risiken dargestellt werden können. So können sich Risiken gegenseitig aufheben (kompensatorischer Effekt) oder sich gegenseitig verstärken (kumulativer Effekt) (vgl. Hartmann 2003: 15). Insbesondere durch die Kumulation vieler kleiner Einzelrisiken kann das Unternehmen in eine existenzgefährdende Situation geraten (so genannter „Dominoeffekt“) (vgl. Romeike 2003: 156). Diese kumulierten Risiken sind oftmals auch die Ursache vieler Unternehmenskrisen. Daher sollte innerhalb der Risikobewertung neben den Einzelrisiken zusätzlich auch das aggregierte Gesamtrisiko des Unternehmens ermittelt werden, wobei die Risikotragfähigkeit nicht überschritten werden darf. Dabei ist zu beachten, dass das aggregierte Unternehmensrisiko nicht gleich der Summe der Einzelrisiken



sein muss (vgl. Seidel 2002: 47). Nur im Idealfall entspricht die Summe auch dem aggregierten Unternehmensrisiko.

Eine unternehmensweite Risikoaggregation ermöglicht insbesondere der Value-at-Risk. Dieser in der Banken- und Versicherungsbranche bereits erprobte und vielfach angewendete Ansatz bestimmt den maximalen Verlust, der mit einer gegebenen Wahrscheinlichkeit (z. B. 95 %) im Rahmen eines vorher festgelegten Zeitraums eintritt (vgl. Dahms 2003: 226). Theoretisch lassen sich mit diesem Bewertungsmodell sämtliche Risiken über alle Unternehmensebenen hinweg erfassen und verarbeiten. Eine Quantifizierung von Chancen erfolgt mit dem Value-at-Risk jedoch nicht (vgl. Weber/Weißberger/Liekweg 1999: 26). Allerdings ergibt sich mit dem Value-at-Risk auch ein hoher Zeit- und Arbeitsaufwand. Die Verwendung der Risikomatrix gestaltet sich dahingehend wesentlich einfacher. Weitere Unterschiede zwischen dem Value-at-Risk und der Risikomatrix können aus dem Anhang 2 entnommen werden.

Die Genauigkeit der Risikoquantifizierung ist jedoch auch stark von der jeweiligen Risikoart abhängig. Während sich finanzielle Risiken (z. B. Zins- und Wechselkursschwankungen) relativ leicht und sicher messen lassen, ist dies bei anderen Risiken wie beispielsweise einem Image- oder Vertrauensverlust erheblich schwieriger (vgl. Neubeck 2003: 84). Die Schäden, die sich daraus ergeben, können in der Regel nur basierend auf den Opportunitätskosten für zukünftig entgehende Gewinne bewertet werden (vgl. Romeike 2003b: 196). Eine Alternative zur Quantifizierung stellt die **qualitative Beurteilung** dar, auch wenn diese oftmals stark subjektiv geprägt ist. So können Risiken beispielsweise in hohe, mittlere und geringe Risiken kategorisiert werden (vgl. Wolf 2004: 213). Es ist auch eine Betrachtung von Best- und Worst-Case-Szenarien sinnvoll (vgl. Diederichs/Form/Reichmann 2004: 193).

Zu berücksichtigen ist zudem, dass Risiken von jeder Person unterschiedlich wahrgenommen werden, so dass immer ein gewisses Maß an Subjektivität vorhanden ist. Diese variierende Risikowahrnehmung kann ihrerseits wieder unterschiedliche Handlungsmaßnahmen der Personen in Bezug auf das Risiko bewirken (vgl. Brebeck/Herrmann 1997: 387).

Hinzu kommt eine Chancenbewertung. Diese sollte nach den gleichen Grundsätzen, wie sie im Rahmen der Risikobewertung Anwendung finden, erfolgen. Von einer Saldierung von Chancen und Risiken sollte jedoch strikt abgesehen werden. Dadurch würde die Gefahr bestehen, einzelne Aspekte in ihrer Wirkung zu verkennen (vgl. Wolf 2002: 1730).

Bei einer Gegenüberstellung von Chancen und Risiken sollte jedoch das Ergebnis der Chancenbewertung das der Risikobewertung übertreffen. Nach erfolgtem wertmäßigen Abgleich lässt sich schließlich der Bedarf an Maßnahmen feststellen, die der Unternehmenszielerreichung dienen (vgl. Kirchner 2003: 16).

Doch bevor die einzelnen Steuerungsmaßnahmen vorgestellt werden, gilt es, die bewerteten Risiken und Chancen an die verantwortlichen Entscheidungsträger zu kommunizieren, die dann die entsprechenden Gegenmaßnahmen einleiten sollen.

#### 5.1.4. Risikokommunikation

Zur Sicherung der Funktionsfähigkeit des gesamten Risikomanagementprozesses ist vor allem eine Risikokommunikation unerlässlich. Risikokommunikation bedeutet eine **zielgerichtete, zeitnahe** und **verdichtete** Weitergabe von Informationen über festgestellte Risiken und Chancen an die relevanten Interessengruppen. Dem Kommunikationsprozess wird dementsprechend eine Filterfunktion zugewiesen, die es ermöglicht, die **richtigen Informationen** zum **richtigen Zeitpunkt** an die **richtige Person** weiterzuleiten. Zum **richtigen Zeitpunkt** bedeutet in diesem Fall, dass die Informationsvermittlung so rechtzeitig zu erfolgen hat, dass noch geeignete Maßnahmen zu ergreifen sind (vgl. Baumeister/Freisleben 2003: 34f). Die **Verdichtung** der Information findet bereits bei der Risikobewertung statt, wo man versucht für einzelne Bereiche oder für das gesamte Unternehmen ein aggregiertes Risiko zu ermitteln (vgl. Weber/Weißenberger/Liekweg 1999: 30).

Um die bewerteten Risiken an die **richtigen Entscheidungsträger** für entsprechende Steuerungsmaßnahmen weiterzuleiten, ist es erforderlich Schwellenwerte einzurichten. Mit Hilfe dieser Schwellenwerte ist eine bessere Zuteilung der Verantwortlichkeit gegeben. Sie werden bereits im Rahmen der Risikostrategie festgelegt. Im Fall des Überschreitens entscheidet eine nächst höhere Instanz über entsprechende Risikosteuerungsmaßnahmen. Dies dient dazu, übergeordnete Stellen nicht informatorisch zu belasten und erst bei Überschreiten der Schwellenwerte Informationen an die höheren Instanzen weiterzugeben (vgl. Vogler/Engelhard 2000: 1429).

Da das Risikomanagement vor allem auch der Führungsunterstützung dienen soll, gehört insbesondere die Geschäftsführung zu den relevanten Interessengruppen der Risikoinformationen (vgl. Neubeck 2003: 86). Die Unternehmensleitung wird vor allem über diejenigen Risiken informiert, die existenzbedrohende Ausmaße für das Unternehmen annehmen können oder schwerwiegende Verlustpotenziale in sich bergen.<sup>6</sup> Dabei sollte das Risikoreporting in das allgemeine Reporting integriert werden, um eine übersichtliche, konsistente, redundanzfreie und effiziente Darstellung zu ermöglichen (vgl. Wolf 2004: 212). Der Nutzen solch einer **regelmäßigen Risikoberichterstattung** liegt darin, dass fortlaufend zu treffende Entscheidungen der Unternehmensführung unter Beachtung einer allgemeinen Risikoeinschätzung erfolgen können (vgl.

---

<sup>6</sup> Vgl. Vogler/Gundert (1998: 2381f), sowie Hornung/Reichmann/Diederichs (1999: 320f).

Seidel 2002: 304) und eine bewusste Reaktion auf Änderungen der Risikolage somit frühzeitig möglich ist, um den Fortbestand des Unternehmens zu sichern (vgl. Neubeck 2003: 87f).

Als Rückkopplung gibt die Risikoberichterstattung auch Informationen über die erfolgten Gegensteuerungsmaßnahmen, so dass die Risikokommunikation den gesamten Risikomanagementprozess fortwährend begleitet (vgl. Weber/Weißberger/Liekweg 1999: 16).

Damit neu auftretende, risikobehaftete Veränderungen – insbesondere bei einer weiten Berichtsfrequenz – nicht zu spät im Unternehmen kommuniziert werden, muss neben der regelmäßigen Berichterstattung auch ein **Ad-hoc-Berichtswesen** vorgesehen werden (vgl. Liekweg 2003: 326). Hiernach hat derjenige, in dessen Verantwortungsbereich eine bedeutende Änderung auftritt, nach Maßgabe der Wesentlichkeitsgrenzen seinen unmittelbaren Vorgesetzten oder gegebenenfalls eine noch höhere Instanz umgehend zu informieren.

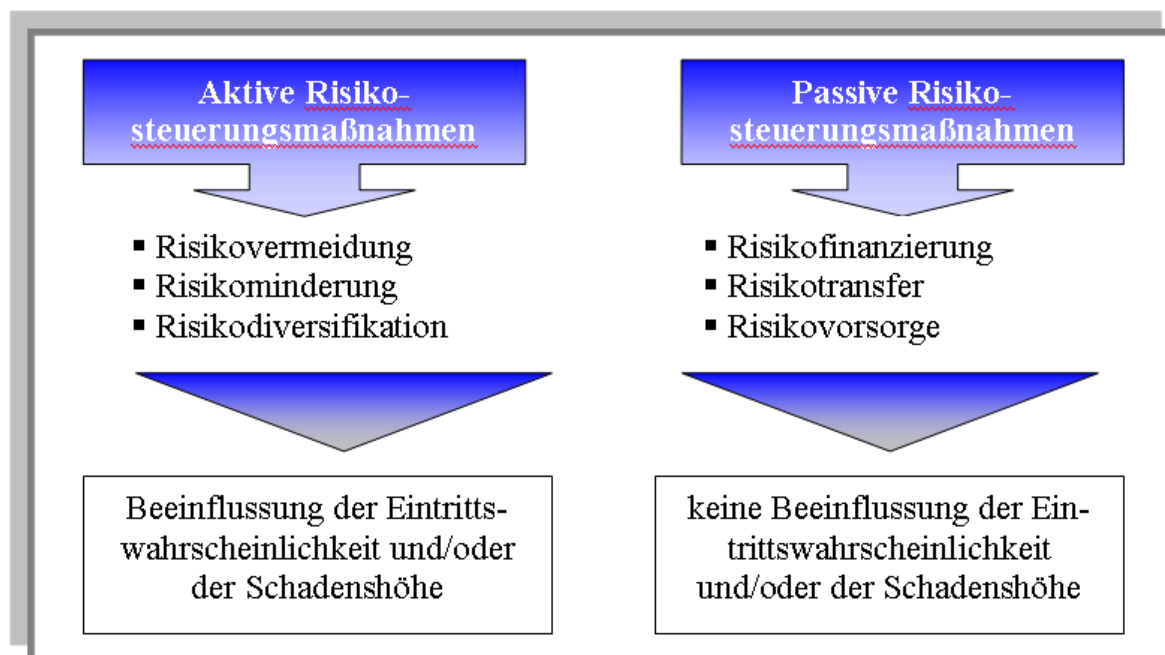
Wurden die relevanten Informationen an die entsprechenden Entscheidungsträger kommuniziert, besteht ihr Aufgabenbereich nun darin, entsprechende Steuerungsmaßnahmen einzuleiten.

#### 5.1.5. Risikosteuerung

Risikosteuerung bedeutet nicht die Beseitigung aller betrieblichen Risiken (vgl. Romeike 2003a: 175), sondern sie hat die Aufgabe, das allgemeine Unternehmensrisiko so zu reduzieren, dass die bestehende Verlustgefahr für die Unternehmung keine Existenzgefährdung mehr darstellt und Chancen überwiegend erhalten bleiben (vgl. Weber/Weißberger/Liekweg 1999: 32).

Die Basis für die Risikosteuerung in einem Unternehmen bildet die Risikostrategie, da auf ihrer Grundlage zu entscheiden ist, welche Risiken akzeptiert werden, weil ihnen entsprechend große Chancen gegenüberstehen und welche Risiken aktiv gesteuert werden sollen (vgl. Seidel 2002: 68). Im Hinblick auf die Steuerung können prinzipiell mehrere Möglichkeiten unterschieden werden, die grundsätzlich in aktive und passive Risikosteuerungsmaßnahmen unterteilt werden können (siehe Abbildung 9). Eine optimale Risikosteuerung ist dabei diejenige, die durch die Risikooptimierung nicht nur den Unternehmensfortbestand sichert, sondern auch den Wert eines Unternehmens steigert.

Abbildung 9: Risikosteuerungsmaßnahmen



Quelle: In Anlehnung an Romeike (2003: 236).

So zielt beispielsweise eine **aktive Risikopolitik** darauf ab, Risiken zu vermeiden, zu vermindern oder zu diversifizieren. Dabei wird versucht, die Risikostrukturen eines Risikos durch eine Verringerung der Eintrittswahrscheinlichkeit und/oder der Schadenshöhe zu verändern (vgl. Zellmer 1990: 53). Die Reduzierung entweder der Eintrittswahrscheinlichkeit oder aber der Schadenshöhe setzt wiederum voraus, dass überhaupt die Möglichkeit zur Beeinflussung des Risikos besteht, wie bereits aus Abschnitt 5.1.3. hervorgegangen ist.

Die „radikalste“ Maßnahme des aktiven Risikomanagements ist die **Risikovermeidung** (vgl. Romeike 2003a: 172). Hierunter ist das gänzliche Ausschalten des Risikos zu verstehen, wobei die Eintrittswahrscheinlichkeit oder die Schadenshöhe auf Null reduziert werden. Hier wird beispielsweise auf die Herstellung eines Produktes mit hohen Produkthaftungsrisiken verzichtet. Dies ist auf der einen Seite zwar eine sehr nahe liegende Strategie des Risikomanagements. Sie führt jedoch auch dazu, dass potenzielle Chancen vermieden werden (vgl. Weber/Weißberger/Liekweg 1999: 34). Aus diesem Grund ist eine Gegenüberstellung der Chancen so wichtig, da ansonsten bedeutende Chancenpotenziale verloren gehen. Die Maßnahme der Risikovermeidung wird im Normalfall nur dann ergriffen, wenn das Risiko keine andere Möglichkeit zulässt, d. h. wenn sich das Risiko in der oberen rechten Ecke der Risikomatrix befindet und keine anderen effektiven Maßnahmen zur Verfügung stehen oder wenn die Chance im Vergleich zum Risiko sehr gering ist (vgl. Kajüter 2003: 63).

Eine weitere Form des aktiven Risikomanagements stellt die **Risikominderung** dar, bei der die Eintrittswahrscheinlichkeit oder die Schadenshöhe von Risiken auf ein akzeptables Maß verringert werden. Risiken können z. B. durch personelle Maßnahmen (Mitarbeiterschulung), durch technische Maßnahmen (Virenschutzprogramme) oder durch organisatorische Maßnahmen (Qualitätsmanagement) vermindert werden (vgl. Hölscher 2002: 15).

Eine Alternative zur Risikominderung stellt die **Risikodiversifikation** dar, welche ebenfalls zu den aktiven Steuerungsmaßnahmen zählt. Ein Risiko wird hierbei in mehrere, voneinander unabhängige Teilrisiken mit gleicher Eintrittswahrscheinlichkeit und geringerer Schadenshöhe aufgeteilt, in dem ein interner Risikoausgleich stattfindet (vgl. Hölscher 2002: 15). Voraussetzung hierfür ist, dass die Risiken weitestgehend voneinander unabhängig sind. So gibt es z. B. die regionale Risikodiversifikation bei der sensible Unternehmensbereiche räumlich voneinander getrennt werden. Beispielsweise werden an verschiedenen Orten gleichartige Produktionsstätten betrieben. Eine personenbezogene Diversifikation hat wiederum das Ziel, den kompletten Ausfall wichtiger Personengruppen im Unternehmen zu verhindern, z. B. durch getrennte Reisen (vgl. Hölscher 2002: 15). Die Risikodiversifikation bietet eine sehr kostengünstige Möglichkeit, Risiken zu vermindern, sofern sie nicht zu stark miteinander korrelieren.

Für das aktive Risikomanagement können letztlich keine allgemeingültigen Vorgehensweisen formuliert werden, da sich die Unternehmen deutlich voneinander unterscheiden und viele Möglichkeiten zur Einwirkung auf Risiken existieren. Jedes Unternehmen bei dem Handlungsbedarf besteht, muss daher individuelle Maßnahmen ergreifen und ein unternehmensspezifisches Instrumentarium entwickeln.

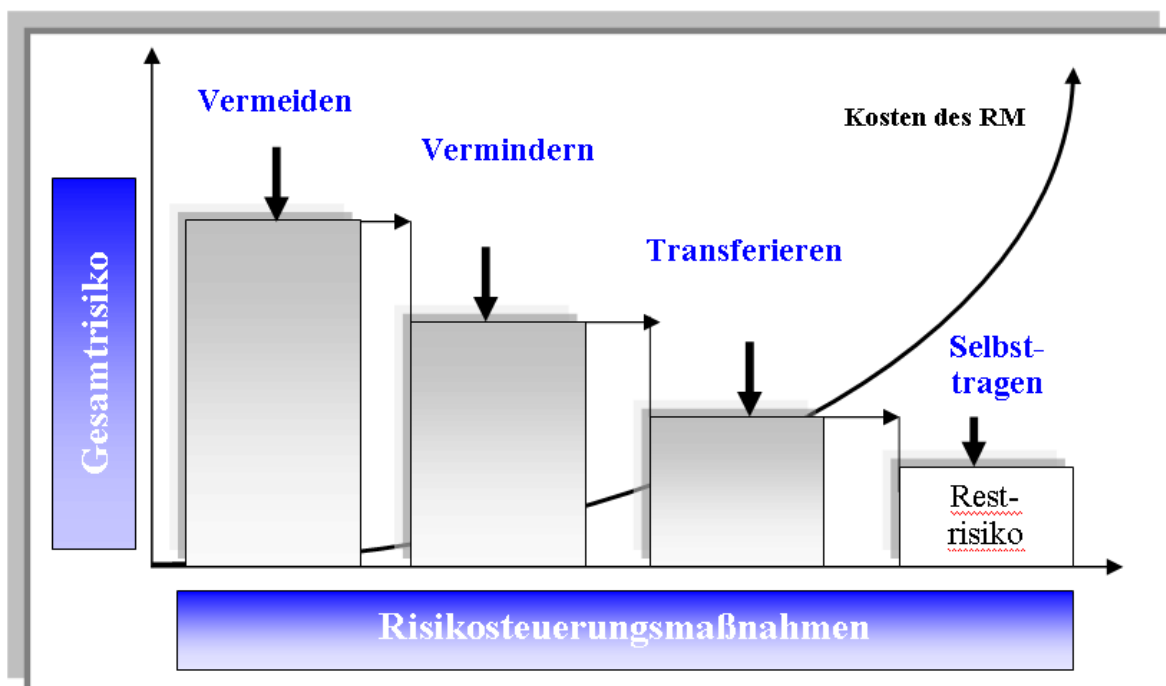
Im Gegensatz zu den aktiven Steuerungsmaßnahmen, die direkt an der Eintrittswahrscheinlichkeit und am Schadensausmaß ansetzen, bleiben die Risikostrukturen von den **passiven Maßnahmen** des Risikomanagements unberührt (vgl. Hölscher 2002: 15). Hier wird der Eintritt eines Risikos bewusst akzeptiert. Das passive Risikomanagement betrachtet alle Risiken, bei denen die Instrumente des aktiven Risikomanagement nicht anwendbar sind bzw. bei denen ihre Anwendung ökonomisch nicht vertretbar ist. Die Zielsetzung des passiven Risikomanagements besteht darin, für entsprechende Risikodeckungsmassen zu sorgen, falls es zu einem Risikoeintritt kommt. Dabei können die passiven Maßnahmen in die Bereiche Risikotransfer, Risikofinanzierung und Risikovorsorge aufgeteilt werden. Beim **Risikotransfer** werden unbekannte Kosten eines Risikos auf Dritte übertragen (vgl. Gleißner 2000: 1625). Ziel ist es, insbesondere die Risiken zu transferieren, die die Finanzkraft des Unternehmens übersteigen. Der traditionelle Weg des Risikotransfers stellt die Versicherung dar (vgl. Zellmer 1990: 62). Bei neueren Methoden werden Risiken beispielsweise auf den Kapitalmarkt transferiert und durch

Finanzderivate abgesichert (vgl. Maier 2001: 24). Aber auch durch die Optimierung von Verträgen mit Lieferanten und Kunden (z. B. Transportrisiken) (vgl. Gleißner 2000: 1625) oder die Inanspruchnahme von Factoring (vgl. Maier 2001: 14) können Risiken transferiert werden.

Können die finanziellen Folgen nicht auf professionelle Risikoträger transferiert werden, so muss das Unternehmen die notwendige Liquidität und die ertragsmäßigen Belastungen aus dem eigenen Finanzsystem bereitstellen. Die Methoden zum Aufbau einer finanziellen Vorsorge sind vielfältig. Als Risikodeckungsmassen können laufende Cashflows, stille Reserven oder Rücklagen dienen (= **Risikofinanzierung/-vorsorge**) (vgl. Hölscher 2002: 15).

Insbesondere im Bereich der Bagatellrisiken, bei denen Nutzen und Aufwand der Risikosteuerung in keinem Verhältnis zueinander stehen, muss das Unternehmen das **Risiko selbst tragen (Risikoakzeptanz)** (vgl. Reichmann/Form 2003: 172f). Dies gilt auch für die nach Einsatz anderer Maßnahmen zur Risikosteuerung verbleibenden Restrisiken, wie sie aus Abbildung 10 ersichtlich sind. Diese Restrisiken bedürfen einer weiteren kontinuierlichen Beobachtung durch Frühwarnindikatoren, um bei einer nachhaltigen negativen Veränderung gegensteuern zu können (vgl. Kajüter 2003: 65).

Abbildung 10: Auswirkungen der Risikosteuerungsmaßnahmen



Quelle: In Anlehnung an Bitz (2002: 89).

Eine **Kombination von Risikotransfer und Risikoakzeptanz** bildet die **Risikoteilung**. Hierbei wird das Risiko zwar nicht im Vergleich zur damit verbundenen Chance, wohl aber in Bezug auf die Risikotragfähigkeit des Unter-

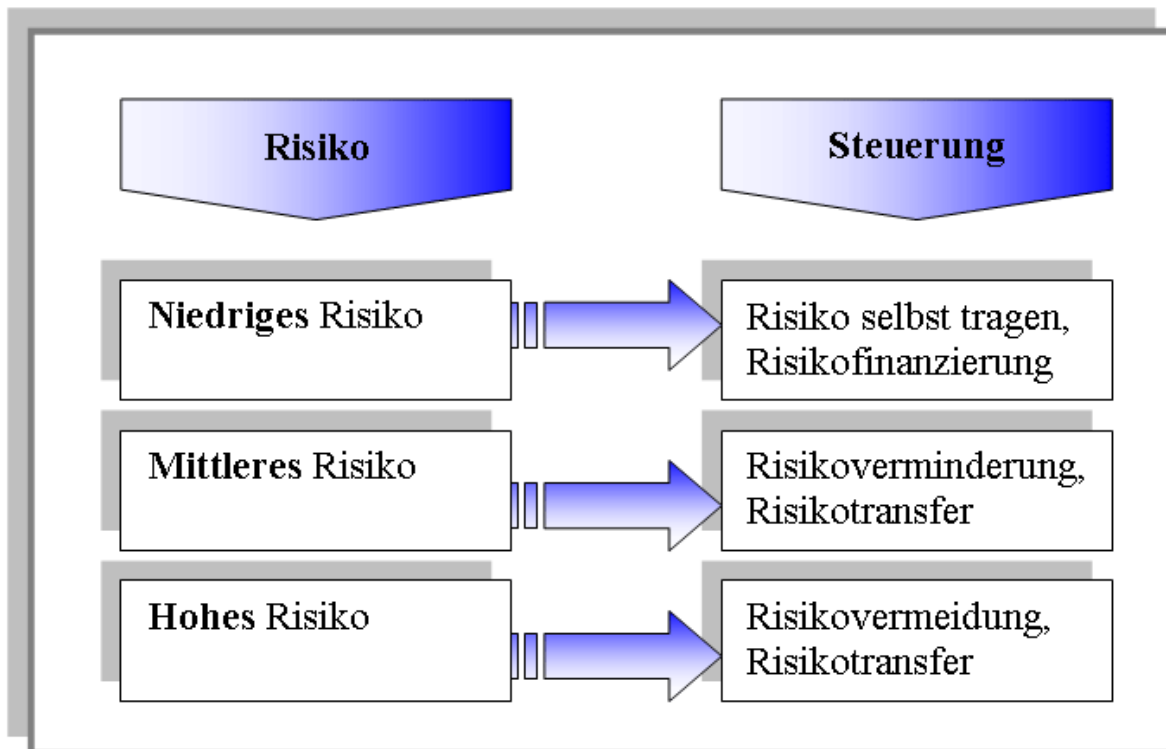
nehmens oder Konzerns als zu hoch angesehen. In diesem Fall bietet die Gründung von Joint Ventures oder anderen Kooperationen die Möglichkeit das Risiko nur anteilig selbst zu übernehmen. Zu bedenken ist, dass auf diese Weise oft neue Risiken entstehen können (z. B. Missbrauch vertraulicher Informationen). Diesen Risiken ist durch entsprechende Vertragsgestaltung entgegenzuwirken (vgl. Kajüter 2003: 65f).

Auch bei der Steuerung von Risiken ist zu beachten, dass zahlreiche Interdependenzen zwischen den Risiken bestehen können. Daher ist beim Einsatz der Steuerungsmaßnahmen stets zu berücksichtigen, dass mit der Verkleinerung eines Risikos auch eine Reduzierung von Chancen einhergehen kann oder mit einer Zunahme anderer Risikoarten verbunden ist. So bewirkt beispielsweise die Ausweitung von Lagerkapazitäten nicht nur die Reduktion des Risikos einer Lieferunfähigkeit, sondern auch die Zunahme des Lagerrisikos.

Die Auswahl der jeweiligen Steuerungsmaßnahmen sollte auch unter Kosten-Nutzen-Überlegungen getroffen werden (vgl. Diederichs/Form/Reichmann 2004: 194).

Eine genormte Zuordnung der Risikosteuerungsmaßnahmen zu den einzelnen Risikoklassen besteht nicht. Jedoch bieten sich folgende Grundüberlegungen zur Wahl der Risikosteuerungsmaßnahmen an:

*Abbildung 11: Zusammenhang Risiko und Steuerungsmaßnahmen*



Quelle: In Anlehnung an Seidel (2002: 301).

Mit der Risikobewältigung ist der Prozess der Risikosteuerung abgeschlossen.

Es ist jedoch wichtig, laufend die Wirksamkeit und die Effizienz des Risikomanagements zu beurteilen, um Ansätze für mögliche Verbesserungen zu identifizieren. Um dies zu gewährleisten, muss im letzten Prozessschritt das Risikomanagement im Unternehmen überwacht werden.

#### 5.1.6. Risikoüberwachung

Die Überwachung des Risikomanagements erfolgt durch eine prozessbegleitende Kontrolle sowie durch eine prozessunabhängige Prüfung. Die **prozessunabhängige Prüfung** ist vor allem Aufgabe der Internen Revision im Unternehmen (vgl. Reichmann/Form 2003: 173). Diese führt als neutrale und unabhängige Instanz interne Prüfungen durch, die sicherstellen sollen, dass der Risikomanagementprozess effizient abläuft und Weisungen eingehalten werden (vgl. Kajüter 2003: 66). Anschließend erstattet sie der Unternehmensführung hierüber Bericht. Die prozessunabhängige Prüfung dient außerdem der kontinuierlichen Weiterentwicklung sowie Verbesserung des Risikomanagements (vgl. Horvath 2003a: 777).

Die **prozessbegleitende Kontrolle** gehört hingegen hauptsächlich zum Aufgabenbereich des Controllings. Es untersucht, ob eingetretene Risiken bekannt waren und ob die Eintrittswahrscheinlichkeiten und Tragweiten der Risiken richtig bewertet wurden (vgl. Weber/Weißenberger/Liekweg 1999: 35). Des Weiteren führt das Controlling Soll-Ist-Vergleiche durch, die die Wirksamkeit der Risikosteuerungsmaßnahmen und die Erreichung der Risikomanagementziele beurteilen sollen (vgl. Horvath 2003a: 782). Da zum Verantwortungsbereich des Controllings nicht nur die Kontrolle des Risikomanagementprozesses gehört, soll im nächsten Abschnitt auf die weiterführenden Aufgaben aufmerksam gemacht werden.

#### 5.2. Risikocontrolling

Institutionell besteht eine enge Verbindung zwischen Risikomanagement und Controlling (vgl. Krystek 1999: 145). Risikomanagement wird in einigen Literaturquellen sogar als Teilfunktion eines umfassenden und fortschrittlichen Controllings beschrieben (vgl. Neubeck 2003: 57).

Grundsätzlich gehört es zur Aufgabe des Controllings, die Unternehmensführung maßgeblich beim Aufbau (systembildend) und der Anwendung (systemkoppelnd) eines individuell geeigneten Risikomanagements und Risikoberichtssystems zu unterstützen (vgl. Martin/Bär 2002: 122). Die Abbildung 12 veranschaulicht die umfassende Funktion des Controllings am Risikomanagementprozess.

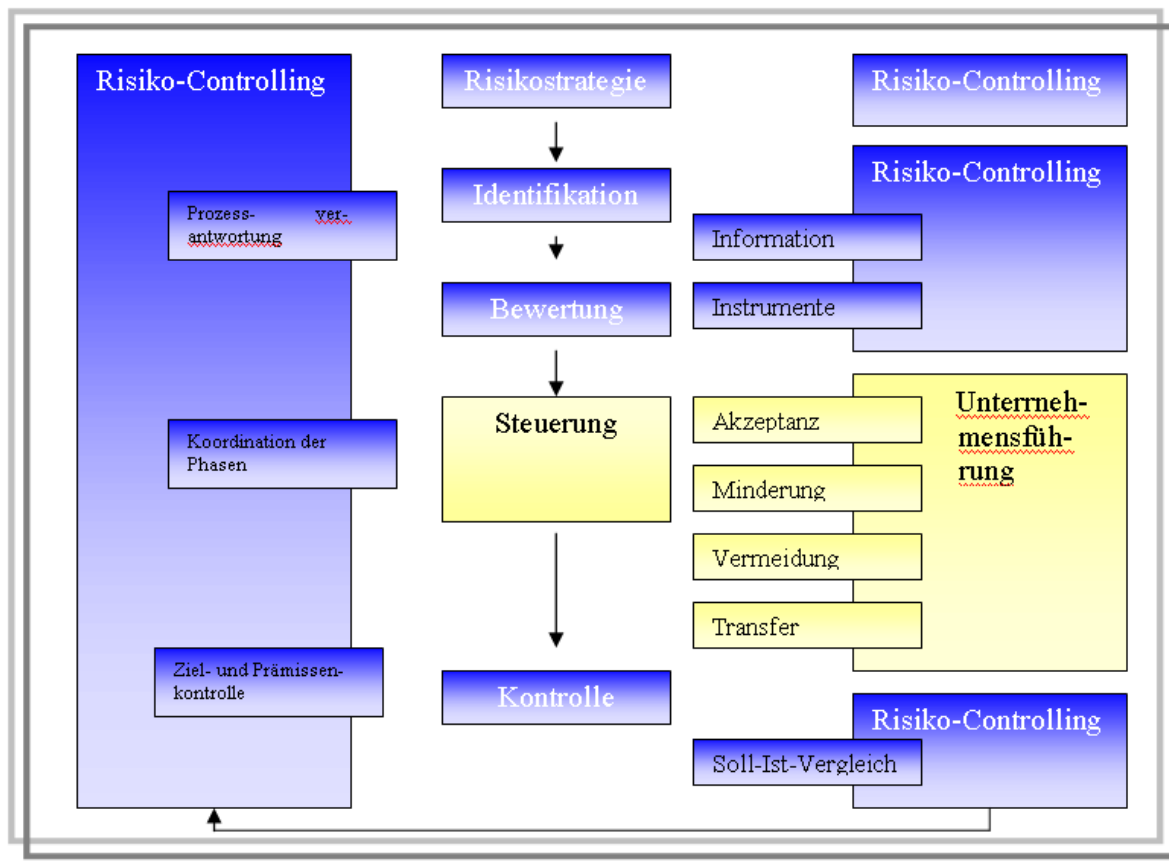
So beginnt die Mitwirkung bereits bei der Ausarbeitung der Risikostrategie in Kooperation mit der Unternehmensleitung (vgl. Martin/Bär 2002: 123). Das Controlling hilft hier bei der Bestimmung der Risikoschwellenwerte, ab denen



bestimmte Gegensteuerungsmaßnahmen getroffen und Verantwortlichkeiten bestimmt werden müssen. Dem Controlling kommt im Risikomanagementprozess auch eine Koordinationsaufgabe zu. So sammelt es alle identifizierten Risiken aus den verschiedenen Bereichen und fasst diese in regelmäßigen Abständen zu einem Risikoinventar zusammen (vgl. Krystek 1999: 147). Dabei prüft es die Interdependenzen zwischen den einzelnen Risiken sowie deren Bewertung hinsichtlich Eintrittswahrscheinlichkeit und Schadenshöhe, um anschließend das aggregierte Gesamtrisiko des Unternehmens zu bestimmen (vgl. Gampenrieder/Greiner 2002: 284). Ziel ist es dabei zu erkennen, ob mögliche Interdependenzen zwischen den Risiken aus verschiedenen Bereichen zu einer Bestandsgefährdung für das Unternehmen führen können. Die ermittelten Erkenntnisse werden dann übersichtlich aufbereitet und an die Geschäftsleitung berichtet (Informationsversorgungsfunktion), die diese Information als Entscheidungsgrundlage für eventuelle Risikosteuerungsmaßnahmen benötigt (vgl. Seidel 2002: 303). Zu dem Aufgabengebiet des Risikocontrollings gehört es zudem, der Geschäftsleitung Maßnahmen vorzuschlagen, die zur Bewältigung der Risiken geeignet sind (Beratungs- und Servicefunktion). Die Auswahl und Steuerung der Maßnahmen obliegt jedoch letztendlich der Geschäftsleitung bzw. dem Management (vgl. Gampenrieder/Greiner 2002: 285).

Abschließend übernimmt das Controlling die Kontrolle über die Wirkung der einzelnen Maßnahmen und führt Soll-Ist-Vergleiche durch, wie bereits im Abschnitt 5.1.6. herausgestellt wurde. Daraus bestimmen sich neue Risikoziele und der Prozess des Risikomanagement beginnt von vorn. Endpunkt wie Ausgangspunkt des Prozesses bildet damit die Risikostrategie (vgl. Weber/Weißberger/Liekweg 1999: 16). Dies unterstreicht die Eigenschaft des Risikomanagementprozesses als Kreislauf.

Abbildung 12: Mitwirkung des Risikocontrollings am Risikomanagementprozess



Quelle: Burger/Buchhart (2002: 58).

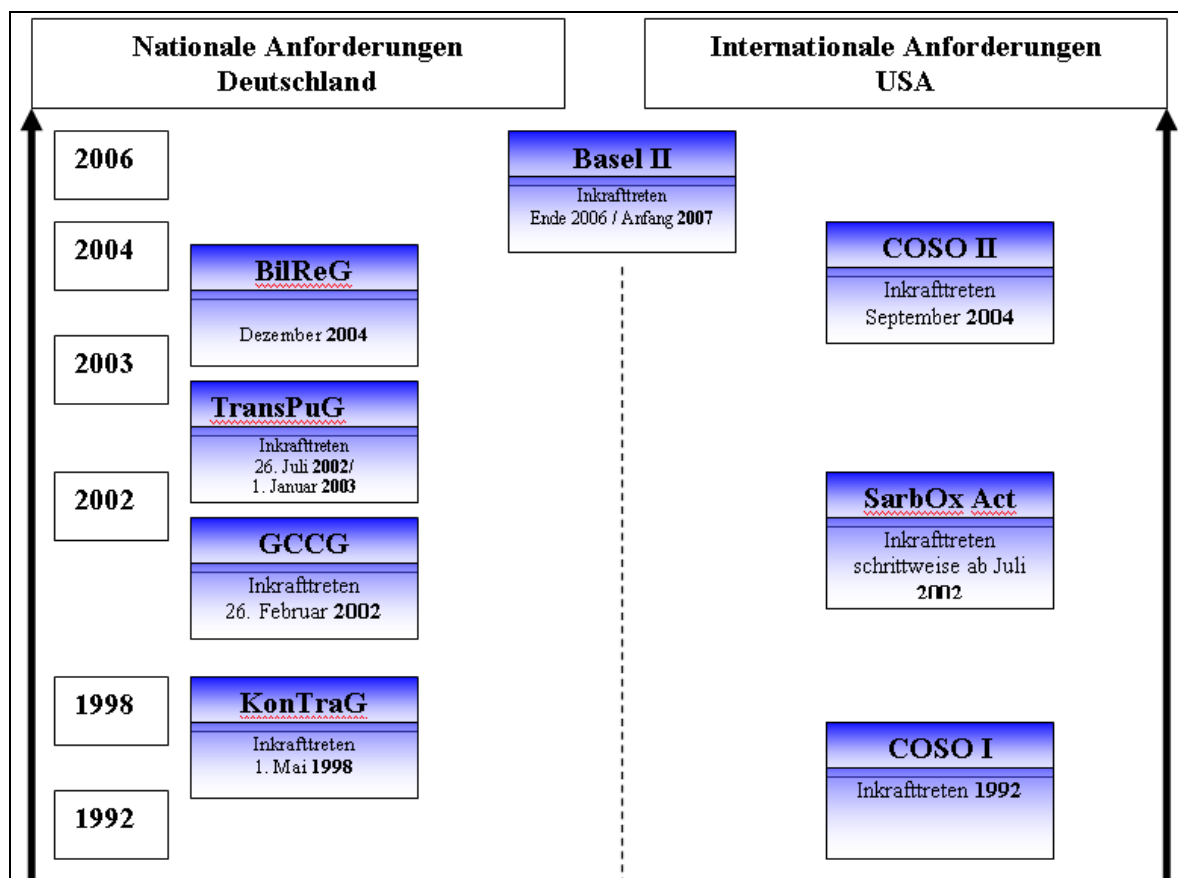
Nach dem nun die grundlegenden Anforderungen an ein betriebswirtschaftliches Risikomanagement dargestellt wurden, gilt es im folgenden Kapitel 6 die nationalen und internationalen Rahmenbedingungen, die die Einführung eines Risikomanagements im Unternehmen zum Teil gesetzlich fordern, empfehlen oder Hilfestellung bei der Ausgestaltung und Implementierung geben, zu untersuchen.

## 6. Externe Anforderungen an ein Risikomanagement

In den letzten Jahren haben insbesondere spektakuläre Unternehmensschieflagen großer Kapitalgesellschaften national wie international die Aufmerksamkeit der Wissenschaft und Praxis auf sich gezogen. Untersuchungen belegen, dass die Gründe der Unternehmenskrisen oftmals in Verhaltensfehlsteuerungen der Unternehmensführung sowie in deren mangelnder Überwachung (vgl. Schöne 2003: 91) zu suchen sind. Die Fehlsteuerungen wiederum entstanden durch unzureichende Kenntnisse und Informationen des Managements über Unternehmens- und Umfeldveränderungen, ein fehlendes Risikobewusstsein

und -management oder durch vorsätzliche Bilanzmanipulationen (vgl. Buderath 2003: 219). Diese Umstände führten dazu, dass insbesondere Kapitalanleger und Kreditgeber verstärkt eine verbesserte Unternehmensführung und -überwachung forderten, was unter anderem auch unter dem Begriff „Corporate Governance“ bekannt ist (vgl. Seidel 2002: 46). Zu einer verbesserten Unternehmensführung gehört unter anderem auch der bewusste und verantwortungsvolle Umgang mit Risiken. Infolgedessen sahen sich Regierung, Wirtschaftsprüfung und privatrechtliche Institutionen gezwungen, hier Handlungsempfehlungen für das Managen von Risiken und für interne Kontrollen im Unternehmen zu geben, von denen einige Gesetzeskraft erlangten (vgl. Buderath 2003: 219) und andere als „Code of Best Practise“ (vgl. Romeike 2003b: 65) zu verstehen sind.

Abbildung 13: Zeitstrahl über die nationalen und internationalen Anforderungen an ein Risikomanagement



Quelle: Eigene Darstellung.

Ziel dieses Kapitels soll es demnach sein, nationale und internationale Rahmenbedingungen, die zur Einführung eines Risikomanagements verpflichten oder dieses empfehlen (siehe Abbildung 13), darzustellen und zu untersuchen, welche Anforderungen sich daraus an ein Risikomanagement ergeben. Da die

Entwicklungen in den USA wie in der Einleitung bereits erwähnt mit COSO als Rahmenwerk für viele internationale Länder eine Vorbildfunktion ausüben, sollen diese stellvertretend für die internationalen Anforderungen stehen.

### 6.1. Nationale Anforderungen

Wie aus Abbildung 12 zu entnehmen ist, wurde in Deutschland das Thema Risikomanagement rechtlich erstmalig 1998 mit dem **Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)** aufgegriffen. Mit dem KonTraG reagierte der Gesetzgeber auf die zahlreich gestiegenen Unternehmensschieflagen und kam damit der Forderung nach einer verbesserten Corporate Governance nach, d. h. einer verantwortungsvolleren Verfassung, Leitung und Überwachung deutscher Unternehmen (vgl. Weber/Weißberger/Liekweg 1999: 39). Dabei handelt es sich beim KonTraG nicht um ein einheitliches Gesetz, sondern um ein Artikelgesetz (vgl. Krystek 1999: 145), bei dem überwiegend bereits bestehende gesetzliche Verpflichtungen, insbesondere des AktG und des HGB, ergänzt und aktualisiert wurden (vgl. Picot 2001: 5). Die größten Veränderungen betreffen dabei Aktiengesellschaften, da die dort eingetretenen Unternehmenskrisen in besonderem Maße die Aufmerksamkeit der Öffentlichkeit auf sich zogen (vgl. Liekweg 2003: 2). Kapitalanleger und Kreditgeber haben vielfach ihr Vertrauen in Unternehmensführung, Aufsichtsrat und Abschlussprüfer verloren und heftige Kritik geäußert (vgl. Böcking/Orth 2000: 242). Infolge der fortschreitenden Globalisierung galt es nun dieses Vertrauen in die deutschen Unternehmen wieder zu stärken und den Finanzstandort Deutschland auch international wettbewerbsfähiger zu machen (vgl. Böcking/Orth 2000: 243). Dies ist notwendig, da sich große Aktiengesellschaften zunehmend international finanzieren und deutsche Emittenten im direkten und weltweiten Wettbewerb mit in- und ausländischen Kapitalnachfragern um die Gunst der potenziellen Anleger stehen. Zudem stellte der Gesetzgeber heraus, dass bei börsennotierten Aktiengesellschaften in zunehmendem Maße eine Kontrolle über die Kapitalmärkte ausgeübt werde (vgl. BT-Drucksache 13/9712: 11) und die Anleger verstärkt Informationen über die Unternehmensführung fordern. Vor diesem Hintergrund geriet das deutsche Aktienrecht und Rechnungslegungsrecht unter starken Modernisierungsdruck und der Gesetzgeber ist mit dem KonTraG dem Wunsch der Anleger nach einer größeren Informationsdichte und -qualität nachgekommen und hat die Pflichten zur Rechnungslegung (**Risikoberichterstattung**, Segmentberichterstattung, Kapitalflussrechnung) erweitert (vgl. Neubeck 2003: 29f), so dass es zu mehr **Transparenz** im Unternehmensbereich kommt (vgl. Schmalenbach-Gesellschaft 2000: 2).

Mit diesen Änderungen beabsichtigte der Gesetzgeber, das deutsche Rechnungslegungsrecht auf die internationalen Finanzmärkte auszurichten (vgl. Brebeck/Herrmann 1997: 381). Dabei erfolgt eine Annäherung an die interna-

tionalen Rechnungslegungsstandards (US GAAP, IAS), bei denen die **Informationsfunktion** und der **Kapitalanlegerschutz** im Vordergrund stehen und nicht der **Gläubigerschutz** und das **Vorsichtsprinzip** wie in der deutschen Rechnungslegung (vgl. Scheffner/Strutz 2002: 203).

Der Gesetzgeber erkannte auch, dass die zahlreichen Unternehmenskrisen überwiegend auf Fehler im Management zurückzuführen sind, das Risiken häufig nicht rechtzeitig erkennt oder gar unterschätzt. So kommt es trotz veränderter Unternehmens- und Umfeldbedingungen zu keiner Anpassung der Unternehmensstrategie, was oftmals Auslöser für eine Unternehmenskrise oder gar die Insolvenz ist, wie bereits in Kapitel 3 erörtert wurde. Daher fordert der Gesetzgeber mit dem KonTraG die Vorstände in § 91 Abs. 2 AktG auf, „geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen **früh** erkannt werden“ (Picot 2001: 12). Aus dieser Neuregelung ist ersichtlich, dass der Gesetzgeber eine Notwendigkeit in der **Einführung eines Risikofrüherkennungs- und Überwachungssystems** hinsichtlich einer guten und verantwortungsvollen Unternehmensführung für unerlässlich hält und Aktiengesellschaften sogar gesetzlich dazu verpflichtet. Die Unternehmensführung soll damit in der Lage sein, kritische Entwicklungen im Unternehmen rechtzeitig wahrzunehmen, um noch geeignete Gegensteuerungsmaßnahmen treffen zu können (vgl. Böcking/Orth 1998: 351).

Mit den Gesetzesänderungen durch das KonTraG zielte der Gesetzgeber auch auf eine Stärkung der von Aufsichtsrat und Abschlussprüfer ausgeübten Kontrollfunktion. Um diesem **Kontrollaspekt** gerecht zu werden, wurde vom Gesetzgeber eine engere Zusammenarbeit zwischen dem Aufsichtsrat und dem Abschlussprüfer beabsichtigt. Des Weiteren wurde der Pflichtenrahmen der Abschlussprüfer auch auf die Prüfung der Risikoberichterstattung und des Risikofrüherkennungssystems erweitert, um das Vertrauen der Anleger weiter zu stärken und die Zahl der Unternehmenskrisen zu verringern.

Welche Forderungen sich aus dem KonTraG in Bezug auf ein Risikomanagement für die Unternehmen im Einzelnen ergeben, soll im Abschnitt 6.1.1. im Vordergrund stehen.

Die Diskussionen um eine verbesserte Corporate Governance hielten auch nach dem KonTraG aufgrund erneuter Unternehmenszusammenbrüche an (z. B. Ph. Holzmann AG) (vgl. Böcking/Orth 2000: 242f). Im September 2001 wurde daraufhin eine Regierungskommission<sup>7</sup> mit der Erstellung eines **German Code of Corporate Governance (GCCG)** beauftragt. Diese Kommission verabschiedete den Kodex am 26. Februar 2002. Dabei enthält der Kodex Vorschriften, Empfehlungen und Anregungen für eine gute und verantwortungsvolle Unternehmensführung, die unter das Prinzip „Comply or Explain“

<sup>7</sup> Neben der Regierungskommission beschäftigten sich noch zwei weitere Gremien mit Corporate Governance. Vgl. Hakelmacher (2001: 178); vgl. Picot (2001: 11).

fallen (vgl. Strenger 2002: 452). Im Gegensatz zum KonTraG ist der German Code of Corporate Governance kein Gesetz, sondern eine Bündelung von Prinzipien und Standards („Best Practice“), denen sich die deutschen börsennotierten Gesellschaften (vgl. Kajüter 2003: 51) im Rahmen einer freiwilligen Selbstverpflichtung unterwerfen (vgl. Strieder 2004: 27). Zwischenzeitlich wurde der Kodex zweimal aktualisiert und die letzte Änderung fand am 21. Mai 2003 statt (vgl. Strieder: 2004: 13). Auch im GCCG wird explizit hervorgehoben, dass der Vorstand für ein angemessenes Risikomanagement und Risikocontrolling im Unternehmen zu sorgen<sup>8</sup> und den Aufsichtsrat regelmäßig, zeitnah und umfassend über Risikolage und Risikomanagement zu informieren hat.<sup>9</sup>

Mit diesem Kodex sollen vor allem zwei Funktionen erfüllt werden. Zum einen sind die zahlreichen Vorschriften des deutschen Corporate Governance-rechtes über mehrere Gesetzestexte verteilt, so dass eine zusammenfassende Darstellung zu mehr Transparenz verhilft (vgl. Horvath 2003a: 824). Zum anderen soll dieser Kodex mit dem Setzen von Standards für eine verantwortungsvolle Unternehmensführung die vorhandenen gesetzlichen Regelungen zusätzlich ergänzen. Hinzu kommt, dass Änderungen im Kodex schneller vorgenommen werden können als bei Gesetzestexten (vgl. Horvath 2003a: 823).

Mit dem **Transparenz- und Publizitätsgesetz (TransPuG)** vom Juli 2002 wurden nun erstmals diese Standards guter und verantwortungsvoller Unternehmensführung aus dem GCCG gesetzlich verankert (vgl. Ettmüller 2003: 690). So haben Vorstand und Aufsichtsrat nach dem neu eingefügten § 161 AktG im Anhang des Jahresabschlusses zu erklären, dass den „Empfehlungen der Regierungskommission Deutscher Corporate Governance Kodex entsprochen wurde und wird oder aber welche Empfehlungen nicht angewendet werden oder wurden“. Der Kodex soll das Vertrauen der Anleger und der Öffentlichkeit in die Leitung und Überwachung deutscher börsennotierter Aktiengesellschaften weiter fördern und damit die Zielsetzungen des KonTraG weiter verfolgen (vgl. Baumeister/Freisleben 2003: 21). Mit dem TransPuG wurden weitere Änderungen oder Ergänzungen im AktG und HGB vorgenommen, auf die im weiteren Verlauf der Arbeit Bezug genommen wird.

Die neueste gesetzliche Grundlage stellt das **Bilanzrechtsreformgesetz (BilReG)** der Bundesregierung vom Dezember 2004 dar, mit dem eine weitere Maßnahme zur Stärkung des Anlegerschutzes dargestellt wird. Mit diesem Gesetz soll vor allem die Abschlussprüfung erneut gestärkt werden. Auch hier werden weitere Veränderungen des AktG und HGB vorgenommen. Auf gesetzliche Änderungen bezüglich des Risikomanagements wird ebenfalls im Laufe dieser Arbeit aufmerksam gemacht.

Aufgrund von **Basel II** entsteht für die Unternehmen eine **mittelbare**

<sup>8</sup> Vgl. GCCG, Fassung vom 21. Mai 2003, S. 7.

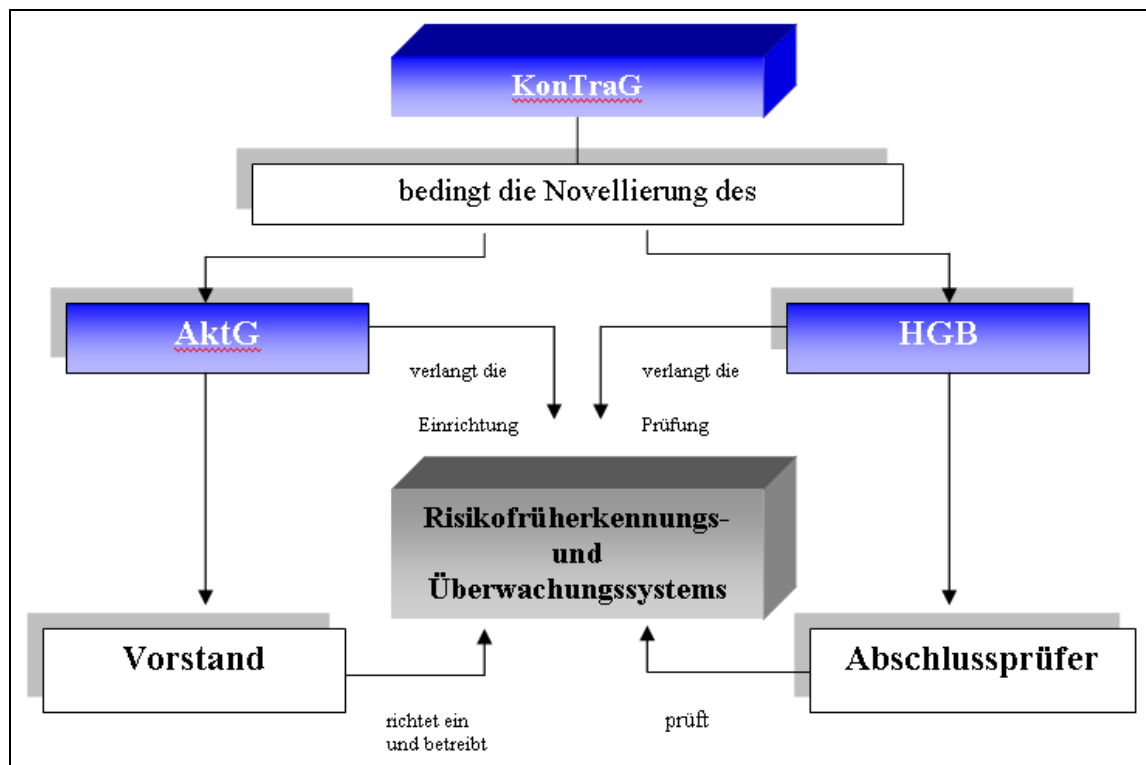
<sup>9</sup> Vgl. GCCG, Fassung vom 21. Mai 2003, S. 5.

„Pflicht“, sich mit einem Risikomanagement auseinanderzusetzen. Banken müssen künftig risikoabhängig Eigenkapital für die Kreditvergabe hinterlegen (vgl. Beinert 2003: 29). Damit soll die Stabilität der Banken gewahrt bleiben und Ausfallwahrscheinlichkeiten verringert werden. Waren es nach Basel I einheitliche 8 Prozent der gesamten Kreditsumme, so hat mit Basel II die Bonität des Kreditnehmers unmittelbare Auswirkung auf das vom Kreditinstitut zu hinterlegende Eigenkapital. Die zusätzlichen Kosten einer erhöhten Unterlegung für die Bank haben in der Folge Auswirkungen auf die Kreditkonditionen in Form von Zinsaufschlägen. Um die Bonität des Kreditnehmers zu prüfen, wird ein Rating durchgeführt, das anhand mehrerer Kriterien zu einer Einschätzung des Unternehmens führt. Ein Kriterium ist unter anderem auch das Vorhandensein eines Risikomanagements im Unternehmen. Ein wirkungsvolles Risikomanagement wirkt sich somit positiv auf das Ratingergebnis aus (vgl. Romeike 2003b: 68). Das Vertrauen der Kreditinstitute in das Unternehmen kann gesteigert werden und dies die Kreditgewährung erleichtern. Das Kreditinstitut muss bei einem weniger risikobehafteten Unternehmen weniger Eigenkapital zur Sicherheit hinterlegen und der Kreditnehmer muss einen geringeren Zins für die Kreditaufnahme zahlen, so dass mit einem effektiven und effizienten Risikomanagement im Unternehmen eine Senkung der Kreditkosten verbunden ist (vgl. Seidel 2002: 104ff). Die Umsetzung von Basel II erfolgt voraussichtlich Ende 2006/Anfang 2007 in nationales Recht (vgl. Beinert 2003: 23f). Obwohl Basel II in dieser Arbeit nur unter den nationalen Rahmenbedingungen aufgeführt wird, so darf daraus nicht geschlossen werden, dass nur Deutschland von Basel II betroffen ist. Wie aus Abbildung 12 ersichtlich, erstrecken sich die Auswirkungen von Basel II auch auf die USA und international auf noch weitere 10 Länder (Belgien, Frankreich, Italien, Luxemburg, Niederlande, Schweden, England, Kanada, Schweiz, Japan) (vgl. Schöne 2003: 91).

#### 6.1.1. „Risikomanagement“ gemäß KonTraG

Da das KonTraG die gesetzliche Ausgangsbasis für die Implementierung eines Risikofrüherkennungs- und Überwachungssystems bildet, sollen die sich daraus für die Unternehmen ergebenden Anforderungen nun im Vordergrund stehen. Dabei beziehen sich die Ausführungen zum KonTraG nur auf diejenigen Regelungen des AktG und HGB, die unmittelbar im Zusammenhang mit dem Risikomanagement stehen. Dazu zählt zum einen die **Einrichtung eines Risikofrüherkennungs- und Überwachungssystems** (siehe Abbildung 14). Der zweite Punkt bezieht sich auf die Verpflichtung, im **Lagebericht** auf die **Risiken der künftigen Entwicklung** einzugehen. Die dritte hier behandelte Regelung bezieht sich auf die **Prüfung des Risikofrüherkennungs- und Überwachungssystem** durch den Abschlussprüfer (siehe Abbildung 14).

Abbildung 14: KonTraG Einführung eines Risikofrüherkennungs- und Überwachungssystems



Quelle: Seidel (2002: 27).

Die Erläuterungen zu den einzelnen gesetzlichen Pflichten unterteilen sich jeweils in Anwendungsbereich und Inhalt. Parallel dazu wird immer auf die neuerlichen Gesetzesänderungen (TransPuG, BilReG) Bezug genommen, so dass die Zusammenhänge besser verdeutlicht werden.

#### 6.1.1.1. Risikofrüherkennungs- und Überwachungssystem

Mit dem durch das KonTraG neu eingeführten **Absatz 2 des § 91 AktG** verpflichtet der Gesetzgeber, wie bereits erwähnt, **Vorstände von Aktiengesellschaften** dazu,

*„geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.“*

##### 6.1.1.1.1. Anwendungsbereich

Die Pflicht zur Einhaltung dieses Gesetzes betrifft gemäß Wortlaut explizit nur Vorstände von Aktiengesellschaften und Kommanditgesellschaften auf Aktien (KGaA), da diese in den unmittelbaren Anwendungsbereich des Aktiengesetzes fallen (vgl. Weber/Weißberger/Liekweg 1999: 41f).

Der Gesetzgeber hat aber bereits in seiner Begründung zur Verabschiedung des Gesetzes auch auf eine Ausstrahlungswirkung auf den Pflichtenrahmen



der Geschäftsführer von Gesellschaften anderer Rechtsformen (z. B. der GmbH und Genossenschaften) (vgl. Zimmer/Sonneborn 2001: 46) in Abhängigkeit von Größe, Komplexität der **Unternehmensstruktur**, sowie **Kapitalmarktzugang**, verwiesen (BT-Drucksache 13/9712: 15). Der Gesetzgeber zielt mit der Ausstrahlungswirkung insbesondere auf solche Gesellschaften, die mit einer AG **strukturell vergleichbar** sind. In der Literatur wird dies von der Existenz eines gesetzlich vorgeschriebenen Aufsichtsrats abhängig gemacht (vgl. Bitz 2000b: 3). Dies wird damit begründet, dass der Gesetzgeber bei der Neuregelung eine bestimmte Organisationsstruktur im Auge gehabt hat, und zwar die Trennung von Leitungs- und Überwachungsorgan (vgl. Hommelhoff/Mattheus 1999: 439). Nach § 77 Abs. 1 BetrVG haben auch GmbHs mit mehr als 500 Arbeitnehmern einen Aufsichtsrat zu bilden. Dies würde bedeuten, dass zumindest GmbHs dieser Größenordnung in den Geltungsbereich der Ausstrahlungswirkung des § 91 Abs. 2 AktG fallen. Nach Hommelhoff/Mattheus sind GmbHs zumindest auch dann von der Verpflichtung des § 91 Abs. 2 AktG betroffen, wenn sie börsengängige Anleihen am Kapitalmarkt platzieren, wobei damit der **Kapitalmarktzugang** als Kriterium eine wichtige Rolle spielt (vgl. Hommelhoff/Mattheus 2000: 221).

Da Tochterunternehmen i. S. d. § 290 HGB Bestandteil eines Konzerns sind und die Pflicht zur Ausgestaltung eines Risikofrüherkennungs- und Überwachungssystems konzernweit zu verstehen ist (vgl. BT-Drucksache 13/9712: 15), fallen auch Tochterunternehmen unter die Anwendung des § 91 Abs. 2 AktG (vgl. Hornung/Reichmann/Diederichs 1999: 318), sofern von ihnen bestandsgefährdende Entwicklungen auf den Mutterkonzern ausgehen können. Beim Mutterunternehmen liegt dann die Überwachungs- und Organisationspflicht (vgl. Bitz 2000b: 2).

#### 6.1.1.1.2. Inhalt

Der Vorstand einer AG (oder einer anderen Gesellschaft je nach Struktur) ist demnach verpflichtet ein Risikofrüherkennungs- und Überwachungssystem einzurichten, auch wenn die Bezeichnung Risikofrüherkennungssystem nicht explizit verwendet wird.

Durch diese Vorschrift konkretisiert der Gesetzgeber die im § 76 Abs. 1 AktG bereits vorhandene und festgelegte allgemeine Leitungsaufgabe des Vorstandes sowie dessen Sorgfaltspflicht nach § 93 Abs. 2 AktG (vgl. Gampenrieder/Greiner 2002: 285). Aufgrund dessen wird in der Literatur häufig die Meinung vertreten, die Pflicht zur Einführung eines Risikofrüherkennungs- und Überwachungssystems habe nur deklaratorischen Charakter und gehöre schon seit jeher zum Aufgabenbereich eines Vorstandes (vgl. Seidel 2002: 46). Dieser Auffassung kann aber anhand zahlreicher Studien entgegen gehalten werden, aus denen hervorgeht, dass Risikomanagement vor der Verabschiedung des KonTraG in den meisten Unternehmen eine eher untergeordnete Rolle spielte und sie oftmals erst das KonTraG zum Anlass der Einfüh-

zung eines solchen Systems genommen haben, um in erster Linie die gesetzlichen Anforderungen zu erfüllen (vgl. Dörner/Bischof 1999: 454ff). Doch auch für Unternehmen, die bereits vor dem Inkrafttreten des KonTraG ein Risikomanagement im Unternehmen eingeführt haben oder in denen andere Instrumentarien zum Umgang mit Risiken (Sicherheitsmanagement, Controlling, Qualitätsmanagement) bereits zur Anwendung kamen, gibt das KonTraG Anlass, diese kritisch zu überprüfen und weiterzuentwickeln.

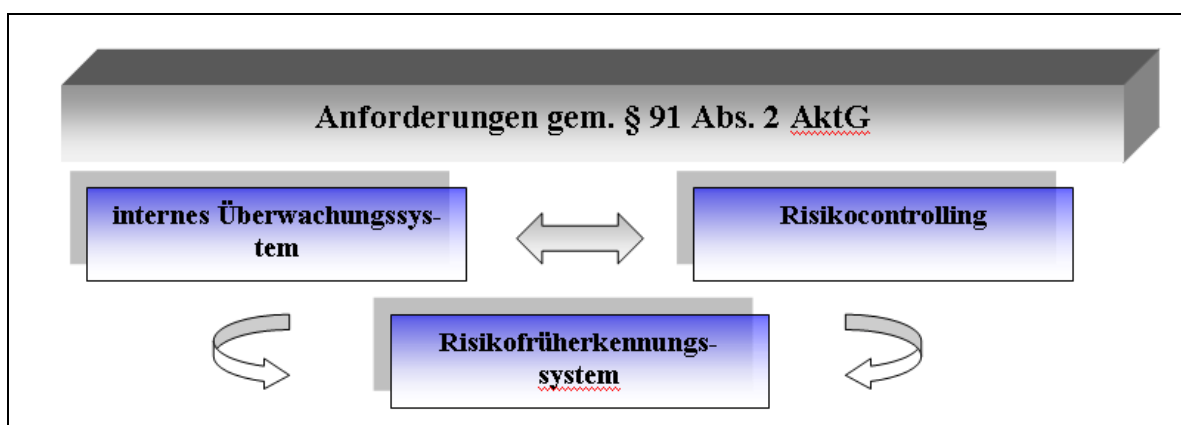
Die Verantwortung des Vorstands zur Risikofrüherkennung wird mit dem KonTraG nun explizit hervorgehoben und führt zweifelsohne zu einer Verstärkung der Pflicht, sich mit Risiken auseinandersetzen zu müssen.

Vorstandsmitglieder, die ihre Pflichten verletzen, sind sogar aus dem daraus eventuell entstandenen Schaden für das eigene Unternehmen (Innenhaftung) als Gesamtschuldner zum Schadenersatz nach § 93 Abs. 2 AktG verpflichtet (vgl. Seidel 2002: 94). Wenn strittig ist, ob ihnen einen Verschulden durch fehlende Sorgfaltspflicht beigemessen werden kann, so trifft die Vorstandsmitglieder die Beweislast (= Beweislastumkehr) (vgl. Bitz 2000b: 4). Auch der Aufsichtsrat soll sich mit dem Risikomanagement der von ihm kontrollierten Unternehmen befassen. Er haftet nach § 116 AktG somit wie der Vorstand.

Allerdings gibt weder der **Gesetzeswortlaut** noch die **Gesetzesbegründung** genauere Angaben, welche konkreten Anforderungen durch § 91 Abs. 2 AktG an den Vorstand gestellt werden. Dies führte in der wirtschaftswissenschaftlichen und juristischen Literatur bis heute zu kontroversen Diskussionen.

Der überwiegende Teil der in der Literatur vertretenen Meinungen schließt aus den Vorgaben, der Gesetzgeber fordere ein **Risikofrüherkennungssystem (Risikofrüherwarnsystem)**, ein **Überwachungssystem** sowie ein **Risikocontrolling** (vgl. insbesondere Lück 1998: 9) (siehe Abbildung 15) und damit kein umfassendes Risikomanagementsystem aus betriebswirtschaftlicher Sicht.

Abbildung 15: Anforderungen gem. § 91 Abs. 2 AktG



Quelle: In Anlehnung an Kirchner (2002: 18).

Dabei ist zu beachten, dass die Elemente in Abbildung 15 zum Teil miteinander

der verbunden sind und nicht eindeutig abgegrenzt werden können. So kann das Controlling Träger von Früherkennungssystemen (Frühwarnsystemen) sein und auch Aufgaben innerhalb des internen Überwachungssystems übernehmen.

Obwohl in der **Gesetzesbegründung** zur Neueinführung des § 91 Abs. 2 AktG, die Vorstandspflicht damit umschrieben wird, für ein „**Risikomanagement**“ zu sorgen, so ist die Formulierung „Risikomanagement“ unpräzise, da der Gesetzgeber gemäß **Gesetzeswortlaut** lediglich ein Risikofrüherkennungssystem fordert. Des Weiteren geht aus der **Gesetzesbegründung** hervor, dass dieses Risikomanagement „**angemessen**“ sein sollte und von der Größe, Branche, Struktur und dem Kapitalmarktzugang (vgl. BT-Drucksache 13/9712: 15) eines Unternehmens abhängig ist. Somit ist ein solches System unternehmensindividuell auszugestalten (vgl. Bitz 2000a: 231), so dass keine konkreten inhaltlichen Vorgaben möglich sind. Es ist offensichtlich, dass die Anforderungen an ein Risikofrüherkennungssystem eines Finanzunternehmens erheblich von denen eines im Bereich der öffentlichen Versorgung tätigen Unternehmens abweichen.

Der Gesetzgeber gibt unter anderem aber auch deshalb keine detaillierten Angaben vor, weil die inhaltlichen Anforderungen des § 91 Abs. 2 AktG unter betriebswirtschaftlichen Aspekten entwickelt werden sollen und die betriebswirtschaftliche Theorie und Praxis auch hier noch zu keiner endgültigen Lösung gefunden hat (vgl. u. a. Vogler 2000: 1425).

Diejenigen, die dem Gesetz nur deklaratorischen Charakter zuweisen, sehen darin den Grund, dass der Gesetzgeber keine Angaben zur Ausgestaltung macht, da die Unternehmen ohnehin bereits über ein Risikofrüherkennungs- und Überwachungssystem verfügen sollten. Dieser Ansatz soll in der vorliegenden Arbeit jedoch nicht verfolgt werden.

Auf Basis des **Wortlauts** des § 91 Abs. 2 AktG wird insbesondere von „geeigneten Maßnahmen“ gesprochen, die vom Vorstand zu treffen sind. Eine nähere Bezeichnung der geeigneten Maßnahmen findet sich im Gesetzestext nicht. Unter Maßnahmen sind deshalb jegliche Handlungen des Vorstands im Rahmen seiner Leitungsaufgaben nach § 76 Abs. 1 AktG zu verstehen, um das im letzten Halbsatz des § 91 Abs. 2 AktG bestimmte Ziel zu erreichen, in dem von der Früherkennung den Fortbestand der Gesellschaft gefährdenden Entwicklungen gesprochen wird (vgl. Zimmer/Sonneborn 2001: 53). Da der Begriff „Gefährdung“ als negative Auswirkung eines „Risikos“ gesehen werden kann, erscheint es als gerechtfertigt, auf Basis des Wortlauts des Aktienrechts von **Risikofrüherkennung** bzw. von **Maßnahmen zur Risikofrüherkennung** zu sprechen, obwohl der Begriff „Risiko“ nicht im Gesetz enthalten ist. Damit liegt der Fokus des Gesetzgebers auf dem Risikobegriff im engeren Sinne sowie auf den reinen Risiken, und die „Chancen“ als Kehrseite des Risikos werden nicht in den Pflichtumfang der Risikofrüherkennungssystems

einbezogen. Diese verlustorientierte Sichtweise des Risikobegriffs entspricht damit der noch eher dem Vorsichtsprinzip geprägten deutschen Rechnungslegung (vgl. Lange 2001: 137). Somit ist auch der Begriff des hier verwendeten Risikofrüherkennungssystems irreführend, da unter der Bezeichnung „Früherkennungssysteme“ eine frühzeitige Ortung von Chancen und Risiken zu verstehen ist (siehe Abschnitt 5.1.2.), so dass hier der Begriff Frühwarnung präziser wäre. Dennoch soll im weiteren Verlauf der Arbeit der Begriff der Risikofrüherkennung angewendet werden, obgleich dies aus betriebswirtschaftlicher Sicht nicht korrekt ist.

Zudem sollte die Identifikation der den fortbestandgefährdenden Entwicklungen **frühzeitig** erfolgen, so dass noch geeignete Maßnahmen zur Sicherung des Unternehmensfortbestands getroffen werden können (vgl. Picot 2001: 12). Als **fortbestandsgefährdende Entwicklungen** werden in der **Gesetzesbegründung** beispielhaft risikobehaftete Geschäfte, Unrichtigkeiten der Rechnungslegung und Verstöße gegen gesetzliche Vorschriften, die einen wesentlich (negativen) Einfluss auf die Vermögens-, Finanz- oder Ertragslage des Unternehmens haben, genannt (vgl. BT-Drucksache 13/9712: 15). Wie bereits erwähnt, können bei Konzernen auch von den Tochtergesellschaften bestandsgefährdende Entwicklungen auf die Mutterunternehmen einwirken, so dass auch diese in das Früherkennungssystem einbezogen werden müssen.

Bestandsgefährdende Risiken zeichnen sich durch ein Schadensausmaß aus, das die Hälfte des vorhandenen Eigenkapitals übersteigt (siehe auch Abschnitt 4.2.). Generell ist dies ein geeignetes Bewertungskriterium bzw. sinnvoller Indikator zur Bestimmung der Grenze für eine Existenzbedrohung. Ein solcher Eigenkapitalverzehr lässt sich auch aus § 92 AktG ableiten, in dem eine Existenzbedrohung bei einem Verlust in Höhe der Hälfte des Grundkapitals unterstellt wird, bei dem der Vorstand zur Einberufung einer Hauptversammlung verpflichtet ist (vgl. Diederichs/Form/Reichmann 2004: 192f).

Angesichts des Gesetzeswortlauts, nur die bestandsgefährdenden Entwicklungen zu erkennen, interpretieren dies einige Autoren dahingehend, dass lediglich existenzbedrohende Einzelrisiken im Rahmen des gesetzlich vorgeschriebenen Risikofrüherkennungssystems zu erfassen sind und eine umfassende Identifikation sämtlicher Einzelrisiken wie sie im betriebswirtschaftlichen Risikomanagement durchgeführt wird, nicht vom Gesetzgeber gefordert ist (vgl. Wall 2002: 11). Demgegenüber stehen allerdings die betriebswirtschaftlichen Erkenntnisse, aus denen hervorgeht, dass auch in ihrer Bedeutung gering einzuschätzende Einzelrisiken kumuliert oder in ihrer Wechselwirkung zu einer Gefahr für den Fortbestand des Unternehmens werden können (vgl. Kindler/Pahlke 2001: 64). Hinzu kommt, dass eine Differenzierung in bestandsgefährdende und sonstige Risiken nicht so einfach möglich ist. Um ein Risiko überhaupt als bestandsgefährdend einzustufen zu können, bedarf es bereits einer betriebswirtschaftlich umfassenden Risikoidentifikation und -be-

wertung sowie der Festlegung von Wesentlichkeitsgrenzen, ab denen ein Risiko als bestandsgefährdend zu klassifizieren ist.

Zum anderen unterstützt der Begriff der gefährdenden „Entwicklungen“ ebenfalls diese Sichtweise. So interpretieren Zimmer/Sonneborn (2001: 51) diesen Begriff dahingehend, dass der Gesetzgeber auf die „Gesamtrisikosituation“ des Unternehmens abstellt. Diese Gesamtrisikosituation resultiert wiederum aus dem Zusammenwirken mehrerer Einzelrisiken, so dass sich vor diesem Hintergrund risikorelevante „Entwicklungen“ nicht abschätzen lassen, ohne die unterliegenden Einzelrisiken zu kennen und in ihrem Zusammenwirken analysiert zu haben (vgl. Wall 2003: 464).

Die Abgrenzung des Gesetzgebers auf bestandsgefährdende Entwicklungen dient insbesondere der Fokussierung des Managements auf besonders kritische Entscheidungsbereiche. Da es sich bei § 91 Abs. 2 AktG um eine Vorstandspflicht handelt und die Maßnahmen zur Früherkennung meist von den operativen Bereichen im Unternehmen durchgeführt werden, ergibt sich auch die Notwendigkeit, die Risiken rechtzeitig an den Vorstand zu kommunizieren.

Aufgrund dieser Gesamtzusammenhänge vertritt insbesondere Frederike Wall die Auffassung, dass ein betriebswirtschaftliches Risikomanagement Voraussetzung für ein „Risikomanagement“ nach KonTraG ist (vgl. Wall 2002: 15). Da jedoch Steuerungsmaßnahmen, verstanden als Reaktionen auf erkannte und analysierte Risiken, nicht zum aktienrechtlich geforderten „Risikomanagement“ gehören (vgl. Zimmer/Sonneborn 2001: 50), kann der Meinung von Frederike Wall nur teilweise gefolgt werden. Ob eine derartige Steuerung vorgenommen oder das Risiko letztendlich vom Unternehmen selbst getragen wird, ist eine Entscheidung des Vorstandes, die unter Zugrundelegung der Sorgfaltspflichten gemäß § 93 Abs. 1 AktG zu treffen ist (vgl. Kajüter 2003: 50). Das Risikofrüherkennungssystem ist damit eher ein Bestandteil eines umfassenden Risikomanagements und beinhaltet zumindest die Teilschritte Risikoidentifikation, -analyse, -bewertung und -kommunikation (vgl. Gampenrieder/Greiner 2002: 285). Demzufolge verlangt § 91 Abs. 2 AktG nicht die Einrichtung eines umfassenden Risikomanagements aus betriebswirtschaftlicher Sicht. Dafür spricht nach Meinung einiger Autoren auch die Tatsache, dass das Gesetz ohne Übergangsregelung in Kraft getreten ist (vgl. Kindler/Pahlke 2001: 66).

Mit der Hervorhebung der Pflicht zur Einführung eines Risikofrüherkennungssystems hat der Gesetzgeber damit Mindestanforderungen für die vom Vorstand zu betreibende Risikofrüherkennung aufgestellt. Geregelt ist damit zumindest das „Ob“, jedoch nicht das „Wie“.

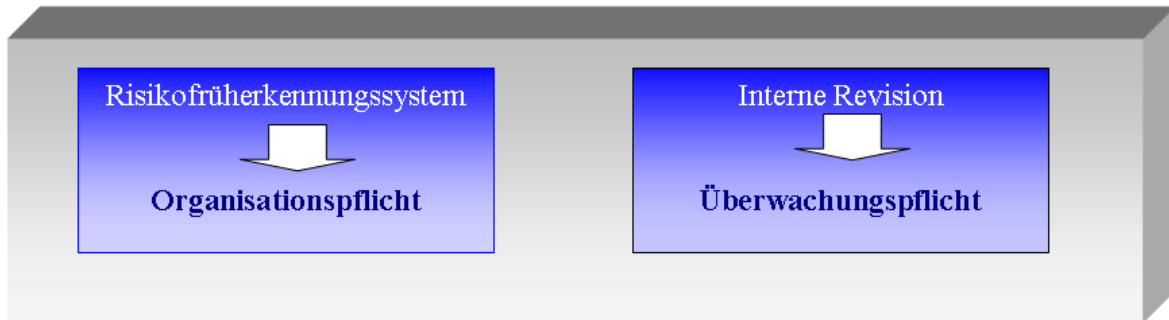
Die von der Betriebswirtschaftslehre und Praxis bislang entwickelten Grundsätze zur Ausgestaltung eines Risikomanagements aus Kapitel 5 schaffen zumindest „Referenzpunkte einer Sorgfaltsbestimmung“. Sie beschreiben zwar nicht verbindlich, welche Maßnahmen ein ordentlicher und gewissenhaf-

ter Geschäftsführer im Rahmen der Risikoerkennung und Risikobewältigung einzuhalten hat, sie können aber als Vergleichskriterien herangezogen werden, um zu beurteilen, ob und wie die tatsächlich ausgeübte Sorgfalt im Einzelfall hätte verbessert werden können (vgl. Kindler/Pahlke 2001: 74).

Schwieriger ist die Interpretation des Einschubs, der den Vorstand im Kontext der Risikofrüherkennung verpflichtet, „insbesondere ein **Überwachungssystem** einzurichten.“ Dabei reicht die Weite der Auslegung in der Literatur von Gleichsetzung mit Früherkennungssystem (vgl. u. a. Weber/Weißberger/Liekweg 1999: 40) bis hin zu einer Verwendung als Oberbegriff für sämtliche interne Überwachungstätigkeiten im Unternehmen. Die Funktion eines Überwachungssystems ist auf der Basis der Bedeutung des Begriffs „Überwachung“ die Beobachtung, ob etwas richtig abläuft, also eine Prüfung und Kontrolle im weitesten Sinne. Durch das Überwachungssystem beobachtet bzw. kontrolliert werden kann in diesem Kontext somit nur das Risikofrüherkennungssystem, d. h. die vom Vorstand eingeleiteten Maßnahmen zur Früherkennung bestandsgefährdender Entwicklungen (vgl. Zimmer/Sonneborn 2001: 55). Aufgrund des allgemein abgeleiteten Verständnisses von Überwachung kann aus dem Gesetz abgeleitet werden, dass der Vorstand die Risikofrüherkennung nicht ausschließlich selbst überwachen soll, sondern durch geeignete interne Maßnahmen für adäquate Prüfungen und Kontrollen der Risikofrüherkennung zu sorgen hat. Praktiziert werden kann dies beispielsweise, indem eine dem Vorstand stabsmäßig angegliederte Interne Revision entsprechende Prüfungen durchführt oder indem durch das Controlling im Unternehmen Kontrollen ausgeführt werden. Vor dem Hintergrund des Wortlauts des Gesetzes und der hierzu vollzogenen Interpretation ist die Bezeichnung „Risikoüberwachungssystem“ bzw. nur „Überwachungssystem“ für die Pflicht der Implementierung von Maßnahmen zur Früherkennung bestandsgefährdender Entwicklungen daher nicht plausibel. Die Überwachung zielt damit nicht auf die Beobachtung von Risiken, sondern auf die Kontrolle bzw. Prüfung der Einhaltung der Maßnahmen zur Risikofrüherkennung ab (vgl. Neubeck 2003: 34). Dies geht auch aus der **Gesetzesbegründung** hervor, in der die Vorstandspflicht mit der Einführung eines **angemessenen Risikomanagements** und einer **angemessenen internen Revision** beschrieben wird. Mit dem Risikomanagement auf der einen Seite und der internen Revision auf der anderen Seite, entspricht dies grundsätzlich der vollzogenen Auslegung gemäß Gesetzeswortlaut bezüglich eines Überwachungssystems. Untermauert wird dies dadurch, dass unter anderem in der Gesetzesbegründung von einer **Organisations- und** auch von einer **Überwachungspflicht des Vorstands (Interne Revision)** gesprochen wird. Die Anordnung auf gleicher Ebene sowie der Hinweis auf eine Interne Revision verdeutlichen die Absicht, dass der Überwachung eine besondere Bedeutung beigemessen wird und eine personelle und organisatorische Unabhängigkeit vom Risikomanagement (bzw. von der

Risikofrüherkennung) vorhanden sein sollte (vgl. Neubeck 2003: 37). Dies steht auch im Einklang mit der im Gesamtkontext des KonTraG vom Gesetzgeber intendierten Verbesserung der Unternehmenskontrolle.

Abbildung 16: Funktion des § 91 Abs. 1 AktG gemäß Gesetzesbegründung



Quelle: Neubeck (2003: 37).

Somit hat das Interne Überwachungssystem besonders auf dem Weg umfassender Prüfungen durch die Interne Revision, die Funktionsfähigkeit des Risikofrüherkennungssystems zu beurteilen und ggf. Verbesserungen anzuregen (Korrekturfunktion).

Funktionsfähige interne Kontrollen sind darüber hinaus in die Arbeitsabläufe zu integrieren, um die Eintrittswahrscheinlichkeit von Fehlern bei der Risikofrüherkennung zu verringern (vgl. Krystek 1999: 147).

In der Gesetzesbegründung konkret angesprochen ist zudem die Notwendigkeit der Existenz eines **Controllings** im Unternehmen, wobei das Controlling verschiedene Aufgaben wahrnehmen kann. Hierbei gehen der Interpretationen der Gesetzesbegründung ebenfalls weit auseinander. So wird von einigen Autoren, die gesetzgeberische Absicht dahingehend gedeutet, dass ein umfangreiches Controlling implementiert werden soll (vgl. Zimmer/Sonneborn 2001: 42). Dem kann hier jedoch nicht gefolgt werden. Das Controlling soll lediglich Teilaufgaben des Risikomanagements durchführen. So kann es an der Risikofrüherkennung (vgl. Krystek 1999: 147) bis hin zur Kontrolle der Maßnahmen der Risikofrüherkennung beteiligt sein, wie bereits in Abschnitt 5.2. dargestellt wurde.

#### 6.1.1.2. Risikoberichterstattung

Neben der Pflicht zur Einführung eines Risikofrüherkennungs- und Überwachungssystems zielte der Gesetzgeber mit dem KonTraG auch auf eine höhere Unternehmenstransparenz ab. So wurde der **§ 289 Abs. 1 HGB** um einen Teilsatz ergänzt:

*„Im Lagebericht sind zumindest der Geschäftsverlauf und die Lage der Kapitalgesellschaft so darzustellen, dass ein den tatsächlichen Verhältnissen entsprechendes Bild vermittelt wird; dabei ist auch auf die Risiken der künfti-*

**gen Entwicklung einzugehen.“**

Gleiches gilt gemäß § 315 Abs. 1 HGB für den Konzernlagebericht. Der Gesetzgeber kam damit der wachsenden Forderung des Kapitalmarktes nach, mehr Informationen über die Unternehmen und Unternehmensentwicklungen zu erhalten (vgl. Kajüter 2001b: 205).

6.1.1.2.1. Anwendungsbereich

Die Pflicht, die Risiken der künftigen Entwicklung im Lagebericht darzustellen, trifft diejenigen Gesellschaften, die einen Lagebericht nach § 289 HGB aufstellen müssen. Die Verpflichtung betrifft damit:

- mittelgroße und große Kapitalgesellschaften (§ 264 Abs. 1 HGB i. V. m. § 267 Abs. 2 und 3 HGB),
- nach PublG rechnungslegungspflichtige Unternehmen (§ 5 Abs. 2 PublG),
- Genossenschaften (§ 336 HGB),
- Kreditinstitute (§ 340 a Abs. 1 HGB) und
- Versicherungsunternehmen (§ 341 a Abs. 1 HGB) (IDW RS HFA 1 1998: 654).

Bei § 267 Abs. 2 HGB ist zu beachten, dass eine Änderung durch den Gesetzgeber mit dem **Bilanzrechtsreformgesetz (BilReG)** vorgesehen ist. Danach werden die Größenklassen für die Definition kleiner Kapitalgesellschaften heraufgesetzt, so dass damit mehr Unternehmen unter die Spezifikation der kleinen Kapitalgesellschaften fallen werden.

6.1.1.2.2. Inhalt

Die Ausweitung des Lageberichts um die Darstellung der Risiken der künftigen Entwicklung war nach der Regierungsbegründung erforderlich, da ansonsten kein den tatsächlichen Verhältnissen entsprechendes Bild über die Lage der Gesellschaft gegeben werden kann (vgl. Picot 2001: 16). Neben der unternehmensinternen Risikokommunikation sollen nun auch detaillierte Informationen über die Risiken nach außen getragen werden. Dieser Risikoberichterstattung misst der Gesetzgeber damit eine wichtige Rolle innerhalb der kapitalmarktorientierten Unternehmenspublizität bei. So wird es in der Begründung zum KonTraG „als wichtig und unabdingbar (...) angesehen, dass der Lagebericht künftig auch Aussagen darüber enthält, mit welchen Risiken die künftige Entwicklung belastet“ ist (vgl. BT-Drucksache 13/9712: 26). Zwar ergibt sich eine Pflicht zur Berichterstattung von Informationen, die Anhaltspunkte über die Risiken im Unternehmen geben, bereits aus der Funktion des Lageberichts selbst. Dennoch hat der Gesetzgeber dies klarstellend als neue Regelung aufgenommen (vgl. Kajüter 2001a: 105).

Die Berichterstattung über diese Risiken kann entweder - analog zu den bereits bestehenden Bestandteilen des Lageberichts - in einem separaten Risikobericht oder als integraler Bestandteil des Wirtschafts- oder Prognoseberichts



erfolgen. Für die erstgenannte Alternative spricht die klare Herausstellung der Risiken, während der Vorteil des integrierten Berichts darin liegt, dass die Gesamtzusammenhänge besser verdeutlicht werden können. Letztendlich beinhaltet der Prognosebericht die erwartete künftige Entwicklung der Gesellschaft, und der Risikobericht stellt mögliche negative Abweichungen vom Prognosebericht dar (vgl. Kajüter 2001a: 105).

Jedoch finden sich weder im Gesetz noch in der Gesetzesbegründung detaillierte Gestaltungsempfehlungen darüber, wie diese Risikoberichterstattung erfolgen soll. Aus dem Wort „einzugehen“ lässt sich nur schließen, dass eine bloße Nennung der Risiken nicht ausreichend ist. Dies hat in der Literatur zu einer intensiven Diskussion um die Interpretation der neuen Regelung geführt (vgl. Dörner/Bischof 1999: 445). Daraufhin hat das Institut der Wirtschaftsprüfer mit der Verabschiedung des Rechnungslegungsstandards zur Aufstellung des Lageberichts (**IDW RS HFA 1**) im Jahr 1998 eine praktische Hilfe gegeben (vgl. Schmalenbach-Gesellschaft 2000: 7). Damit liegt ein Berichtsstandard vor, welcher der Praxis unter anderem auch grobe Anhaltspunkte für die Darstellung der Risiken der künftigen Entwicklung gibt. Das IDW führt in diesem Rechnungslegungsstandard aus, zu welchen Risiken sich die Geschäftsleitung näher zu äußern hat. Die im Lagebericht darzustellenden Risiken können dabei sowohl aus der betrieblichen Tätigkeit als auch aus dem Unternehmensumfeld resultieren (interne und externe Risiken). Die Darstellung sollte sich jedoch aufgrund der Klarheit auf wesentliche Risiken der künftigen Entwicklung beschränken (vgl. IDW RS HFA 1, 1998: 658). Damit sind solche Risiken gemeint, die entweder bestandsgefährdend sind oder einen wesentlichen Einfluss auf die Vermögens-, Finanz- oder Ertragslage haben können. Ob eine Bestandsgefährdung vorliegt, ist wieder abhängig von der Risikotragfähigkeit des Unternehmens (vgl. Dörner/Bischof 1999: 449). Weiterhin ist die Berichtspflicht daraufhin einzuschränken, dass nur auf diejenigen Risiken einzugehen ist, die mit hoher Wahrscheinlichkeit erwartet werden (vgl. IDW RS HFA 1, 1998: 657).

Neben der verbalen Beschreibung dieser Risiken soll auch eine Quantifizierung vorgenommen werden, um das eventuelle Schadensausmaß näher zu bestimmen.

Aus dem Wortlaut des Gesetzes ergibt sich zudem, dass nicht nur die aktuellen, sondern auch die künftigen Risiken zu erfassen sind. Für jeden Abschlussstichtag muss daher auf eine den Verhältnissen dieses Zeitpunkts beruhende, zukunftsbezogene Einschätzung der Existenzfähigkeit des Unternehmens erfolgen. Für bestandsgefährdende Risiken wird aufgrund des inhaltlichen Zusammenhangs mit der Fortführungsprämisse nach § 252 Abs. 1 Nr.2 HGB ein Zeitraum von einem Jahr (vgl. Bitz 2000b: 7), gerechnet ab dem Abschlussstichtag der Berichtsperiode, für zweckmäßig erachtet. Bei der Berichterstattung über sonstige wesentliche Risiken sind hingegen zwei Jahre

zugrunde zu legen (vgl. IDW RS HFA 1, 1998: 658). Sind innerhalb dieser Fristen keine berichtspflichtigen Risiken erkennbar, **kann** dies durch eine Fehlanzeige verdeutlicht werden. Die Angabe einer Fehlanzeige ist jedoch sinnvoll, da die Lageberichtsadressaten sonst nicht erkennen, ob die fehlenden Angaben auf eine unzureichende Berichterstattung zurückzuführen sind oder in der Tat keine berichtspflichtigen Risiken existieren. Nur so wird die Berichterstattung im Lagebericht bzw. im Konzernlagebericht ihrer Informations- und Warnfunktion gerecht.

Insgesamt bestehen für die Praxis mit dem Rechnungslegungsstandard jedoch weiterhin erhebliche Ermessensspielräume für die Risikoberichterstattung. So haben empirische Analysen im Jahr 2000 gezeigt (vgl. Kajüter 2001a: 107ff), dass die Unternehmen diesen Vorgaben des RS HFA 1 nicht folgen. In den wenigsten Lageberichten wurden bestandsgefährdende Risiken dargestellt. Außerdem beschränkten sich die Ausführungen zumeist auf allgemeine externe Risiken, und unternehmensinterne Risiken wurden meist vernachlässigt. Wenn Risiken dargestellt wurden, so mangelte es vor allem bei den Angaben der Eintrittswahrscheinlichkeit sowie einer Quantifizierung.

Diese Ergebnisse haben den dringenden Bedarf an einer weiteren Konkretisierung der Risikoberichtspflicht verdeutlicht. Der DSR (Deutscher Standardisierungsrat) hat dies erkannt und mit dem **DRS 5** (Deutscher Rechnungslegungsstandard) am 29. Mai 2001 einen Vorschlag für die Risikoberichterstattung im **Konzernlagebericht** (§ 315 Abs. 1 HGB) unterbreitet (vgl. Kajüter/Winkler 2004: 249f). Eine analoge Anwendung auf den Lagebericht gem. § 289 Abs. 1 HGB wird jedoch empfohlen (vgl. Kajüter 2001b: 206).

Grundsätzlich betrifft der Rechnungslegungsstandard Mutterunternehmen in der Rechtsform einer Kapitalgesellschaft (§ 290 HGB) sowie der Kapitalgesellschaft gleichgestellte Unternehmen (§ 264 a HGB). Aber auch für Unternehmen, die nach § 11 PubLG zur Konzernrechnungslegung verpflichtet sind, ist der DRS 5 relevant.

Der deutsche Standardisierungsrat ist ein vom BMJ anerkanntes privates Rechnungslegungsgremium, dessen rechtliche Grundlagen und Voraussetzungen durch die Einführung des § 342 HGB mit dem KonTraG geschaffen wurden (vgl. Böcking/Orth 1998: 363f). Diesem Gremium kommen gemäß § 342 HGB folgende grundsätzliche Aufgaben zu:

- Beratung des Bundesministeriums der Justiz bei den die Rechnungslegungsvorschriften betreffenden Gesetzgebungsverfahren (die Konzernrechnungslegung betreffend);
- Entwicklung von Empfehlungen zur Anwendung der Grundsätze über die Konzernrechnungslegung;
- Vertretung der Bundesrepublik in internationalen Standardisierungsgremien (Sitz im Board des IASC als deutscher Vertreter (vgl. Niehus 2001: 53)).

Mit dem DRS 5 formalisiert und konkretisiert der deutsche Standardisierungsrat inhaltlich die gesetzliche Verpflichtung gemäß § 315 Abs. 1 HGB, damit den Adressaten des Konzernlageberichts entscheidungsrelevante und verlässliche Informationen über die Risikolage des Konzerns zur Verfügung gestellt werden. Er ist als branchenübergreifender Standard konzipiert und deshalb bewusst abstrakt formuliert, um ausreichend Flexibilität für die individuellen Erfordernisse der Unternehmen zu gewähren (vgl. Kajüter 2001a: 105). Er geht jedoch über die Anforderungen, die aus dem HGB abgeleitet werden, wesentlich hinaus. Es wird eine separate, weitaus detailliertere Risikoberichterstattung explizit gefordert. Auch im Vergleich mit internationalen Rechnungslegungsstandards werden Regelungen geschaffen, die über den Anforderungen von US-GAAP und IAS liegen. Dort existieren allenfalls teilweise ähnliche explizite Regelungen, aber keine Forderung nach einer abgeschlossenen Risikoberichterstattung (vgl. Kajüter 2001b: 209).

In formaler Hinsicht verlangt der DRS 5 für die Risikoberichterstattung einen separaten, geschlossenen Abschnitt innerhalb des Konzernlageberichts. Einer klaren Abgrenzung der Risikoberichterstattung, auch vom Prognosebericht, wurde somit der Vorzug vor einer integrierten Darstellung eingeräumt.

Der DRS 5 stellt unmissverständlich klar, dass der Schwerpunkt der Berichterstattung auf die internen, unternehmensindividuellen Risiken zu legen ist (vgl. Kajüter 2001a: 110). Dadurch wird der in der Praxis beobachteten Tendenz zur Fokussierung auf die externen Risiken entgegengewirkt. Gleichzeitig trägt diese Regelung dazu bei, dass die externen Adressaten vor allem über solche Risiken informiert werden, die sie selbst in der Regel relativ schwer einschätzen können. Neben den Risiken **kann** zur besseren Darstellung auch über Chancen berichtet werden (vgl. Baumeister/Freisleben 2003: 46). Diese Entwicklung entspricht der bis dahin herrschenden Literaturmeinung. Damit kommt der betriebswirtschaftlich gebräuchliche Risikobegriff hinsichtlich seiner umfassenderen, nämlich beidseitigen Erfassung von Zielabweichungen (= spekulative Risiken), zur Anwendung. Die Berichterstattung über Chancen liegt dabei überwiegend bereits im Eigeninteresse des Unternehmens. Allerdings darf sie nicht die Risiken von untergeordneter Bedeutung erscheinen lassen und damit die Lage des Konzerns verzerrt darstellen. Auf jeden Fall ausgeschlossen ist eine Saldierung von Chancen und Risiken, da so das tatsächliche Gefährdungspotenzial durch den Rechnungslegungsadressaten nicht mehr einschätzbar ist (vgl. Kajüter 2001a: 106) und dadurch ein unzutreffendes Bild der Risikolage hervorgerufen werden kann.

Die Frage der Quantifizierung von Risiken wird im DRS 5 differenziert geregelt. Der DRS 5 verlangt eine Risikoquantifizierung nur dann, wenn dies nach anerkannten und verlässlichen Methoden möglich und wirtschaftlich vertretbar ist und die quantitative Angabe eine entscheidungsrelevante Information für die Adressaten des Konzernlageberichts darstellt. Damit müssen zu-

nächst nur Finanzrisiken quantifiziert werden (z. B. mit statistischen Risikomaßen wie dem Value-at-Risk). In diesem Fall sind die zugrunde liegenden Bewertungsmodelle und deren Annahmen zu erläutern, weil sie das Ergebnis der Risikobewertung stark beeinflussen (vgl. Kajüter 2001a: 106). Zudem sind Risiken nach dem DRS 5 von der Berichtspflicht ausgenommen, wenn bereits Maßnahmen zu ihrer Bewältigung umgesetzt worden sind (vgl. Dörner/Bischof 1999: 447f).

Der DRS fordert darüber hinaus, das vorhandene Risikomanagement im Unternehmen in angemessener Form zu beschreiben. Dabei sind die Strategie, der Prozess und die Organisation zu erläutern.

Der DRS 5 greift damit einige Aspekte auf, die im Rahmen der empirischen Analyse als Mängel bei der Umsetzung des § 315 Abs. 1 HGB identifiziert worden sind.

Damit geht der DRS 5 über die Anforderungen des RS HFA 1 vom IDW hinaus. Er enthält in inhaltlicher und formaler Sicht umfassendere Regeln zur Risikoberichterstattung auf die hier im Detail nicht weiter eingegangen wurde. Durch die formulierten Regeln trägt der DRS 5 jedoch zur Klärung der offenen und teilweise auch strittigen Fragen bei und gibt der Praxis den dringend benötigten Orientierungsrahmen für die Aufstellung der Risikoberichte.

Die praktische Umsetzung erweist sich jedoch auch weiterhin als Problem, da dieser Standard keine Gesetzeskraft hat (vgl. Kajüter 2001a: 111).

Grundsätzlich können die Anforderungen der Rechnungslegungsstandards jedoch nur eingehalten und über die Risiken berichtet werden, wenn im Unternehmen ein Risikofrüherkennungssystem vorhanden ist. Den Vorgaben des § 91 Abs.2 AktG kommt damit gesteigerte Bedeutung zu (vgl. Wall 2003: 461). Die möglichst umfangreiche Risikoidentifikation und -bewertung ist damit dem Risikobericht naturgemäß vorgeschaltet. Daraus ergibt sich, dass sämtliche Unternehmen über ein Risikofrüherkennungssystem verfügen müssen, die zu einer Berichterstattung über die Risiken der künftigen Entwicklung im Lagebericht verpflichtet sind.

Ogleich dies vom Gesetzgeber nicht explizit geäußert, so liegt die Vermutung nahe, dass die Regelungen zur unternehmensbezogenen Risikoberichterstattung und die Forderung nach der Einrichtung eines Risikofrüherkennungs- und Überwachungssystem in einem inneren Zusammenhang stehen, insbesondere vor dem Hintergrund einer beabsichtigten stetigen Annäherung des internen und externen Rechnungs- und Berichtswesens (vgl. Weber/Weißberger/Liekweg 1999: 43).

Um das Vertrauen in die Informationen des Risikoberichts zu erhöhen, unterliegt die Berichterstattung über die Risiken der künftigen Entwicklung der Prüfungspflicht durch einen Wirtschaftsprüfer. So hat der Gesetzgeber den **§ 317 Abs. 2 HGB** um einen Satz 3 ergänzt, in dem es heißt:

*„Dabei ist auch zu prüfen, ob die Risiken der künftigen Entwicklung zutref-*

*fend dargestellt sind.“*

Das Ergebnis der Prüfung ist im Bestätigungsvermerk gem. § 322 Abs. 2 und 3 HGB (**TransPuG**) festzuhalten.

Der Gesetzgeber sieht jedoch mit dem Bilanzrechtsreformgesetz (**BilReG**) eine erneute Änderung der §§ 289 und 317 HGB vor (siehe Anlage 3). Dabei soll die Risikoberichterstattung um eine Chancenberichterstattung ergänzt werden (vgl. Kajüter/Winkler 2004: 250), so dass der Gesetzestext gem. (§ **315 Abs. 1 S. 4 HGB**) § **289 Abs. 1 S. 4 HGB** wie folgt lautet:

*„Ferner sind im (Konzern-)Lagebericht die wesentlichen Ziele und Strategien der gesetzlichen Vertreter (des Mutterunternehmens) für die Kapitalgesellschaft (für den Konzern) zu beschreiben sowie die voraussichtliche Entwicklung mit ihren wesentlichen **Chancen und Risiken** zu beurteilen und zu erläutern; zugrunde liegende Annahmen sind anzugeben.“*

Dieses Gesetz soll erstmals auf nach dem 31. Dezember 2004 beginnende Geschäftsjahre Anwendung finden.

Hinzu kommt eine Neufassung des § **289 Abs. 2 Nr. 2 HGB** sowie analog des § **315 Abs. 2 Nr. 2 HGB**:

*Der Lagebericht soll auch eingehen auf*

- a) die Risikomanagementziele und -methoden der Gesellschaft einschließlich ihrer Methoden zur Absicherung aller wichtigen 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.“*

Durch das BilReG werden damit spezielle Berichtspflichten zu Risiken aus der Verwendung von Finanzinstrumenten in Anlehnung an IAS 32 eingeführt (vgl. Kajüter/Winkler 2004: 260).

Nach § 317 Abs. 2 HGB (**BilReG**) hat der Abschlussprüfer dann künftig auch zu prüfen, *„ob die **Chancen und Risiken** der künftigen Entwicklung zutreffend dargestellt sind“*.

Diese Prüfung soll erstmals bei nach dem 31. Dezember 2004 beginnenden Geschäftsjahren durchgeführt werden.

Durch diese Gesetzesänderungen vollzieht der Gesetzgeber eine bemerkenswerte Korrektur. Die durch das KonTraG eingeführte einseitige Risikoberichterstattung soll durch eine ausgewogene Darstellung von Chancen **und** Risiken abgelöst werden. Auch reicht es nicht mehr aus, auf die voraussichtliche Entwicklung lediglich „einzugehen“, sondern diese auch „zu beurteilen und zu erläutern“. Angesichts der Informationsbedürfnisse der Kapitalmarktakteure erscheint diese Neuausrichtung sinnvoll und entspricht auch der be-

triebswirtschaftlichen Sichtweise. Unternehmerisches Handeln besteht vor allem im Nutzen von Chancen und nicht in der Vermeidung von Risiken. So ist es für den Informationsadressaten auch immer wichtig, welche Chancen den Risiken gegenüberstehen, um ein Urteil über die Unternehmensentwicklung treffen zu können. Aus der zukünftigen Chancenberichterstattung ergibt sich jedoch für den § 91 Abs. 2 AktG eventuell Änderungsbedarf. Es kann nur über Chancen berichtet werden, wenn sie auch identifiziert, analysiert und bewertet werden.

Mit der Forderung Preisänderungs-, Ausfall- und Liquiditätsrisiken darzustellen, ergeben sich keine weiteren Veränderungen, da diese bisher auch schon zu den berichtspflichtigen Risiken zählten. Durch die ausdrückliche Erwähnung im Gesetz wird die Bedeutung, die diesen Risiken in der Praxis häufig zukommt, jedoch nochmals besonders hervorgehoben.

#### 6.1.1.3. Prüfung des Risikofrüherkennungs- und Überwachungssystems

Einen wesentlichen Bestandteil des KonTraG bildet auch die Erweiterung und qualitative Verbesserung der gesetzlichen Jahresabschlussprüfung. Im vorhergehenden Abschnitt wurde bereits auf die Prüfung der Risikoberichterstattung aufmerksam gemacht. Um dem Kontrollaspekt des KonTraG noch stärker gerecht zu werden, wurde im HGB der § 317 auch noch um folgenden Absatz 4 ergänzt (vgl. Picot 2001: 13):

*„Bei einer Aktiengesellschaft, die Aktien mit amtlicher Notierung ausgegeben hat, ist außerdem im Rahmen der Prüfung zu beurteilen, ob der Vorstand die ihm nach § 91 Abs. 2 des Aktiengesetzes obliegenden Maßnahmen in geeigneter Form getroffen hat und ob das danach einzurichtende Überwachungssystem seine Aufgaben erfüllen kann.“*

##### 6.1.1.3.1. Anwendungsbereich

Diese Regelung des KonTraG betrifft damit nur Aktiengesellschaften, die Aktien mit amtlicher Notierung an einer Wertpapierbörse ausgegeben haben. Aktien gelten im Sinne dieser Vorschrift als amtlich notiert, wenn sie im Börsensegment „Amtlicher Handel“ geführt werden. Nicht amtlich notiert sind Aktien der Segmente „Geregelter Markt“, „Neuer Markt“ und „Freiverkehr“.

Dieser Anwendungsbereich stieß jedoch in der Praxis und Öffentlichkeit auf Unverständnis, da gerade Unternehmen am „Neuen Markt“ erhöhten Risiken ausgesetzt sind und dort eine Notwendigkeit zur Prüfung des Risikofrüherkennungssystems besteht (vgl. Schindler/Rabenhorst 2001: 161).

Mit dem Transparenz- und Publizitätsgesetz (**TransPuG**) im Juli 2002 vollzog der Gesetzgeber dann eine Änderung des **§ 317 Abs. 4 HGB** (siehe Anlage 3) und ersetzte die Wörter *„Aktiengesellschaft, die Aktien mit amtlicher Notierung ausgegeben hat“* durch *„börsennotierte Aktiengesellschaft“* und erweiterte damit die Prüfungspflicht auf mehr Unternehmen (vgl. Baumeister/Freisleben 2003: 25). Als börsennotiert sind Gesellschaften nach § 3 Abs.2

AktG anzusehen, wenn deren Aktien an einem von staatlich anerkannten Stellen geregelt und überwacht, regelmäßig stattfindenden und für das Publikum mittelbar zugänglichen Markt gehandelt werden. Damit wird die bisherige und mit der Zielsetzung einer erhöhten Transparenz und Kontrolle im Unternehmensbereich nicht konsistente Beschränkung auf Gesellschaften, die in dem Marktsegment des Amtlichen Handels nach den §§ 36 ff. BörsG n.F. notiert werden, aufgehoben und der Anwendungsbereich des § 317 Abs. 4 HGB auf eine größere Bandbreite von Aktiengesellschaften ausgedehnt (vgl. Neubeck 2003: 173ff). Danach sind nun auch insbesondere Aktiengesellschaften von der Pflicht zur Prüfung des Risikofrüherkennungssystems betroffen, deren Aktien in den Segmenten „Geregelter Markt“ und „Neuer Markt“ gehandelt werden sowie Aktiengesellschaften, die (ausschließlich) in einem entsprechenden ausländischen Kapitalesegment notiert sind. Alle anderen Aktiengesellschaften sind befreit. Aus der Befreiung von der Prüfungspflicht resultiert jedoch keine Befreiung von der Pflicht, ein Risikofrüherkennungssystem nach § 91 Abs. 2 AktG einzurichten.

Bei den Gesellschaften, für die keine Pflichtprüfung existiert, kann jedoch der Aufsichtsrat auf freiwilliger Basis den Abschlussprüfer beauftragen, das Risikofrüherkennungs- und Überwachungssystem in die Abschlussprüfung einzubeziehen (vgl. Baumeister/Freisleben 2003: 25). Die Ziele einer derartigen freiwilligen Prüfung liegen insbesondere im Versuch einer Vertrauenssteigerung der Jahresabschlussadressaten in das Unternehmen.

Von einer mittelbaren Prüfung kann gesprochen werden, wenn Prüfungshandlungen, die sich zunächst nicht auf das Risikofrüherkennungs- und Überwachungssystem beziehen, Auslöser für dessen Prüfung werden. Dieser Fall ist insbesondere bei der Prüfung des Risikoberichts nach § 317 Abs. 2 S. 2 HGB zu erwarten, da ohne ein funktionierendes System der Risikofrüherkennung die Verlässlichkeit und Vollständigkeit im Ausweis wesentlicher Risiken der künftigen Entwicklung nicht sichergestellt ist (vgl. Picot 2001: 28).

#### 6.1.1.3.2. Inhalt

Demnach hat der Abschlussprüfer das im Unternehmen implementierte und betriebene Risikofrüherkennungs- und Überwachungssystem zu prüfen. Damit unterliegen die Aktionen aus dem § 91 Abs. 2 AktG nicht nur einer internen Überwachung, sondern auch einer externen Prüfung. Diese beschränkt sich auf eine System- („Maßnahmen in geeigneter Form getroffen“) und Funktionsprüfung („seine Aufgaben erfüllen kann“) und umfasst keine Geschäftsführungsprüfung (vgl. Lehner/Schmidt 2000: 268).

Der Abschlussprüfer soll lediglich zu einem Urteil darüber gelangen, ob die erforderlichen Maßnahmen zur Risikofrüherkennung und zur Einrichtung eines Überwachungssystems getroffen wurden und ob diese Maßnahmen für das Unternehmen zweckentsprechend und wirksam waren. Weiterhin ist zu untersuchen, ob das Risikofrüherkennungs- und Überwachungssystem während des

gesamten zu prüfenden Zeitraums bestanden hat (vgl. Vogler/Engelhard 2000: 1427).

Daraus wird deutlich, dass eventuell vorgenommene Risikosteuerungsmaßnahmen im Unternehmen nicht Gegenstand der Prüfung sind (vgl. Böcking/Orth 2000: 249). In der allgemeinen Öffentlichkeit besteht stattdessen häufig die Vorstellung, dass diese ebenfalls in den Prüfungsbereich des Wirtschaftsprüfers gehören und damit sichergestellt ist, dass die Unternehmen verantwortungsvoll mit ihren Risiken umgehen (= Erwartungslücke) (vgl. Wiedmann 1998: 342). Diese Überprüfung fällt jedoch in die Aufgabenbereiche des Aufsichtsrates, des Controllings sowie der internen Revision.

Über das Ergebnis der Prüfung ist nach § 321 Abs. 4 HGB in einem gesonderten Teil des Prüfungsberichts zu informieren und anzugeben, ob Verbesserungen des Risikofrüherkennungs- und Überwachungssystems notwendig sind. Festgestellte Mängel sind zwingend in den Prüfungsbericht aufzunehmen (vgl. Baumeister/Freisleben 2003: 19f). Eine Darstellung des Risikofrüherkennungssystems und konkrete Verbesserungsvorschläge im Falle einer Mängelfeststellung müssen jedoch nicht in den Prüfungsbericht aufgenommen werden (vgl. Picot 2001: 29).

Da jedes Unternehmen individuelle Maßnahmen zur Früherkennung von Risiken treffen muss, ist es für den Abschlussprüfer notwendig, sich unternehmensspezifische Kenntnisse anzueignen. Nur so ist er in der Lage, eine sachgerechte Prüfung und Einschätzung durchzuführen.

Anders als bei der Jahresabschlussprüfung, bei der der Abschlussprüfer Sachverhalte mit gesetzlichen oder außergesetzlichen Normen vergleicht, fehlt bei der Beurteilung der Maßnahmen zur Risikofrüherkennung ein entsprechendes gesetzlich fixiertes Sollobjekt (vgl. Brebeck/Herrmann 1997: 390 und Schindler/Rabenhorst 2001: 161). Ein Grund hierfür liegt in der Notwendigkeit, dass ein „Risikomanagement“ unternehmensindividuell auszugestalten ist (vgl. Brühwiler 2001: 117).

Für viele Wirtschaftsprüfungsgesellschaften ergeben sich jedoch gerade daraus erhöhte Gewinnchancen, die sie mit der Entwicklung von unternehmensspezifischen Risikomanagementkonzeptionen und Beratungsleistungen erzielen können. Diese Tatsache wirft jedoch die Frage auf, ob damit die Neutralität des Abschlussprüfers noch gewährleistet ist und nicht die Eigeninteressen im Vordergrund stehen. So wird die Wirtschaftsprüfungsgesellschaft immer ein Risikomanagement empfehlen, das letztendlich in der Prüfung einfach zu handhaben ist. Damit rückt die optimale Ausgestaltung des Risikomanagements für das Unternehmen in den Hintergrund.

Schließlich wurden durch das Institut der Wirtschaftsprüfer (IDW) generelle Anforderungen an die Gestaltung eines „Risikomanagements“ im Unternehmen identifiziert, die als Orientierungsrahmen für das fehlende Sollobjekt dienen können und entsprechend fallspezifisch konkretisiert werden müssen.



Diese wurden schließlich im Jahre 1999 im PS 340 (Die Prüfung des Risikofrüherkennungssystems nach § 317 Abs. 4 HGB) zusammengefasst (vgl. IDW PS 340 1999: Ziff. 1-3). Mit diesem Prüfungsstandard wurden damit indirekt Mindestanforderungen an ein Risikofrüherkennungssystem gestellt, die nun im nächsten Abschnitt erläutert werden sollen.

#### 6.1.2. „Risikomanagement“ gemäß IDW PS 340

Wie aus dem vorhergehenden Abschnitt ersichtlich wurde, haben in Deutschland die Abschlussprüfer laut KonTraG zu überprüfen, ob der Vorstand geeignete Maßnahmen zur Früherkennung von bestandsgefährdenden Entwicklungen getroffen hat.

Da der Gesetzgeber keine weiteren Ausführungen zur Ausgestaltung der geeigneten Maßnahmen zur Risikofrüherkennung gemacht hat, entwickelte das Institut der Wirtschaftsprüfer einen Prüfungsstandard PS 340, der als Grundlage für die nach § 91 Abs. 2 AktG geforderten Pflichten herangezogen werden kann (vgl. Hohnhorst 2002: 98).

Auch das Institut der Wirtschaftsprüfer verwendet den in der Gesetzesbegründung zum § 91 Abs. 2 AktG ebenfalls aufgeführten Begriff „Risikomanagement“. Im Gegensatz zur Gesetzesbegründung wird im entsprechenden Prüfungsstandard IDW PS 340 der Begriff jedoch präzisiert. Risikomanagement wird als „Gesamtheit aller organisatorischen Regelungen und Maßnahmen zur Risikoerkennung und zum Umgang mit Risiken unternehmerischer Betätigung“ (IDW PS 340 1999: Ziff. 2 (3)) definiert. Im gleichen Kontext wird jedoch klargestellt, dass die Reaktionen des Vorstandes oder anderer Entscheidungsträger und damit die Steuerung von Risiken nicht als Maßnahmen im Sinne von § 91 Abs. 2 AktG gelten. Wie bereits im Laufe der Arbeit herausgestellt wurde, umfasst § 91 Abs. 2 AktG mit dem Risikofrüherkennungs- und Überwachungssystem demnach nur einen Teilaspekt des gesamten Risikomanagementsystems, auf den sich auch nur der Prüfungsumfang erstreckt (vgl. Seidel 2002: 56). Das im Prüfungsstandard bestimmte Risikofrüherkennungssystem gilt als wichtiger Bestandteil des Risikomanagementsystems und umfasst dem Wortlaut des Prüfungsstandards zufolge die (rechtzeitige) Erfassung, die Analyse und die Kommunikation bestandsgefährdender Entwicklungen (vgl. IDW PS 340 1999: Ziff. 2 (5)). Zur Abgrenzung des Prüfungsumfanges des Abschlussprüfers muss also zwischen Risikofrüherkennungssystem und Risikomanagementsystem unterschieden werden.

##### 6.1.2.1. Komponenten des „Risikomanagements“

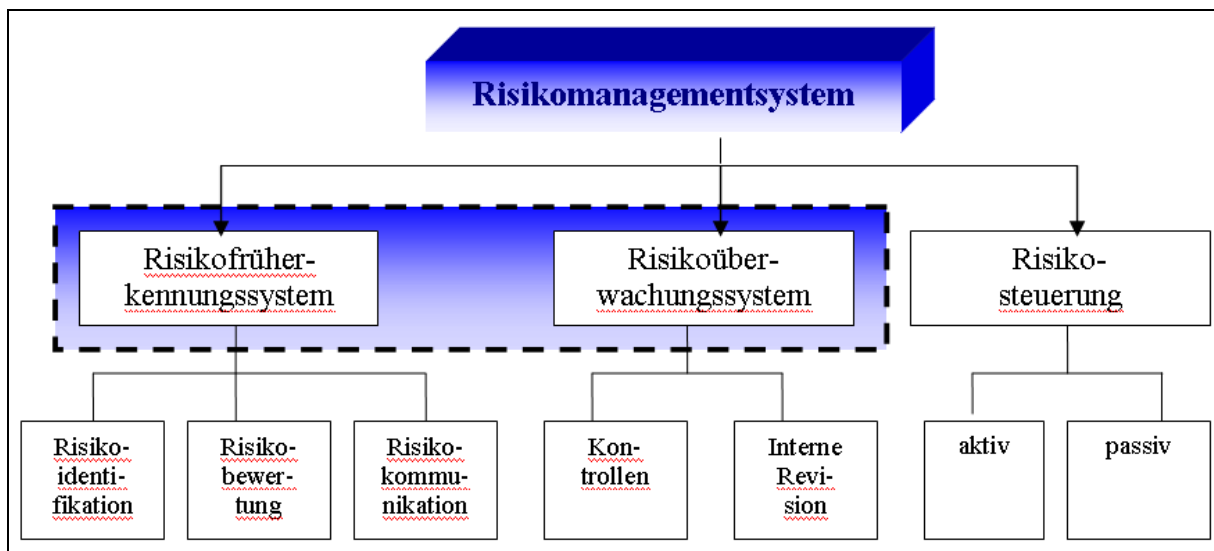
Ein Risikofrüherkennungssystem laut § 91 Abs. 2 AktG umfasst gemäß IDW demnach folgende Teilsaspekte eines gesamten Risikomanagementsystems:

- Risikoidentifikation (IDW: Risikoerkennung)
- Risikobewertung: (IDW: Risikoanalyse)
- Risikokommunikation: (IDW: Risikokommunikation)
- Risikoüberwachung (IDW: Einrichtung eines Überwachungssystems)<sup>265</sup>

Risikofrüh-  
erkennungssystem

Die einzelnen Bestandteile werden in Abbildung 17 noch einmal grafisch veranschaulicht.

Abbildung 17: Risikomanagement im Verständnis des IDW



Quelle: In Anlehnung an Martin/Bär (2002: 87).

Laut IDW ist jede unternehmerische Betätigung aufgrund der Unsicherheit künftiger Entwicklungen mit Chancen und Risiken verbunden. Unter Risiko ist dabei „allgemein die Möglichkeit ungünstiger künftiger Entwicklungen zu verstehen“ (IDW PS 340 1999: Ziff. 2). Nach der Definition des IDW sind Risiken damit Gefahren eines Vermögensverlustes im Sinne einer Wertminderung des Eigenkapitals oder einer Verschlechterung der Finanz- und Ertragslage des Unternehmens. Dabei stellt auch das IDW gem. § 91 Abs. 2 AktG auf den negativen Teil des Risikos ab und lässt Chancen bei der Betrachtung außen vor.

Nach dem **IDW PS 340** sind folgende Komponenten und Maßnahmen zur Erfüllung der Pflicht nach § 91 Abs. 2 AktG erforderlich:

#### 6.1.2.1.1. Festlegung der Risikofelder

Zunächst sind diejenigen Risikofelder festzulegen, die zu bestandsgefährdenden Entwicklungen führen können. Dabei ist zu beachten, dass Risiken aus

sämtlichen Unternehmensbereichen resultieren können und es daher notwendig ist, alle betrieblichen Prozesse und Bereiche einer Untersuchung auf Risiken, die den Unternehmensfortbestand gefährden können, zu unterziehen. Dabei sind auch Wechselwirkungen zwischen den einzelnen Risiken zu beachten, aus denen sich auch eine Bestandsgefährdung ergeben kann. Schließlich folgt eine Abgrenzung derjenigen Unternehmensbereiche, aus denen solche Risiken in besonderem Maße hervorgehen bzw. auf die externe Risiken besonders einwirken. Dieser Vorgang hat unternehmensindividuell zu erfolgen und darf nicht als einmaliger Prozess verstanden werden, sondern muss laufend wiederholt und überprüft werden (vgl. IDW PS 340 1999: Ziff. 3.1).

#### 6.1.2.1.2. Risikoerkennung und Risikoanalyse

Um die Wirksamkeit der Risikoerkennung zu gewährleisten, muss sichergestellt werden, dass nicht nur bereits vordefinierte Risiken, sondern auch unbekannte und latente Risiken erkannt werden. Eine wichtige Voraussetzung dafür ist die Schaffung einer Risikokultur im Unternehmen. Besonders in den vorher festgelegten risikobehafteten Unternehmensbereichen ist ein stark ausgeprägtes Risikobewusstsein der dort tätigen Mitarbeiter unerlässlich.

Nachdem die Risiken erkannt wurden, gilt es sie einer Risikoanalyse/-bewertung zu unterziehen, bei der die Beurteilungskriterien Eintrittswahrscheinlichkeit und quantitative Auswirkung zur Anwendung kommen. Zu berücksichtigen sind auch hier wieder eventuell vorhandene Interdependenzen zwischen den Einzelrisiken. Außerdem sind Risiken einer weiteren Beobachtung zu unterziehen, bei denen bereits Gegensteuerungsmaßnahmen eingeleitet wurden (vgl. IDW PS 340 1999: Ziff. 3.2).

#### 6.1.2.1.3. Risikokommunikation

Da ein Ziel des KonTraG unter anderem in der Verbesserung der Informationsversorgung der Unternehmensleitung liegt, sieht auch das IDW in der regelmäßigen Berichterstattung, insbesondere über alle nicht bewältigten Risiken, an den Vorstand eine zentrale Bedeutung für die Funktionsfähigkeit des Risikofrüherkennungssystems. Dies wiederum setzt eine Kommunikationsbereitschaft bei den verantwortlichen Stellen voraus. Hinzu kommt eine Definition von Schwellenwerten für bestandsgefährdende Risiken, deren Überschreiten eine Berichtspflicht auslöst. Schließlich muss auch die Risikokommunikation so angelegt sein, dass Wechselwirkungen zwischen Risiken (Kumulation) aus unterschiedlichen Unternehmensbereichen hinreichende Berücksichtigung finden. Des Weiteren muss es möglich sein, neben der periodischen Kommunikation auch eilbedürftige Informationen unmittelbar an die Geschäftsleitung weiterleiten zu können, ohne dass die vorgesehenen Berichtswege eingehalten werden müssen (Ad-hoc-Berichterstattung) (vgl. IDW PS 340 1999: Ziff. 3.3).

#### 6.1.2.1.4. Zuordnung von Verantwortlichkeiten und Aufgaben

Es ist sicherzustellen, dass in den jeweiligen Unternehmensbereichen Verantwortlichkeiten für Risiken festgelegt werden. Diese Maßnahme soll gewährleisten, dass die Risiken erfasst, bewältigt und kommuniziert werden. Insbesondere soll ein Kommunikationsaustausch zwischen den einzelnen Unternehmensbereichen stattfinden, damit Wechselwirkungen zwischen Risiken erkannt werden. Die Verantwortung für den Informationsaustausch sollte dabei den jeweiligen Berichtsempfängern zugewiesen werden, damit es zu einer rechtzeitigen Erfassung der Risiken kommt (vgl. IDW PS 340 1999: Ziff. 3.4).

#### 6.1.2.1.5. Einrichtung eines Überwachungssystems

Eine wichtige Voraussetzung für das Funktionieren eines Risikofrüherkennungssystems ist, dass die eingerichteten Maßnahmen auch „gelebt“ werden. Dies zu überprüfen ist nicht nur Gegenstand der Abschlussprüfung, sondern Aufgabe eines internen Überwachungssystems. Eine Überwachung kann dabei einerseits durch prozessintegrierte Kontrollen erfolgen (z. B. durch eine Überwachung der Einhaltung von Meldegrenzen oder durch eine computergestützte Überwachung der Einhaltung von Berichtsterminen), aber andererseits auch durch prozessunabhängige Prüfungen durchgeführt werden (z. B. durch die interne Revision). Die interne Revision nimmt innerhalb des Unternehmens hinsichtlich des Risikofrüherkennungssystems insoweit eine vergleichbare Aufgabe wahr wie der externe Abschlussprüfer, indem sie die wirksame Umsetzung der getroffenen Maßnahmen überprüft (vgl. IDW PS 340 1999: Ziff. 3.5).

Gegenstand der Prüfungstätigkeit der internen Revision können laut IDW u. a. folgende Aspekte sein:

- „vollständige Erfassung aller Risikofelder des Unternehmens,
- Angemessenheit der eingerichteten Maßnahmen zur frühzeitigen Risikoerfassung und Risikokommunikation
- kontinuierliche Anwendung der Maßnahmen,
- Einhaltung der integrierten Kontrollen“ (IDW PS 340 1999: Ziff. 3.5).

Das Vorhandensein einer internen Revision hat für den Wirtschaftsprüfer den Vorteil, dass er auf die Resultate der erfolgten Prüfungen der internen Revision zugreifen kann.

#### 6.1.2.1.6. Dokumentation der getroffenen Maßnahmen

Laut IDW ist es notwendig, die Maßnahmen, die zur Erfüllung des § 91 Abs. 2 AktG eingerichtet wurden, ausreichend in einem so genannten Risikomanagementhandbuch zu dokumentieren. Art und Umfang der Dokumentation sind dabei von der Größe und Komplexität des Unternehmens abhängig. Aus der Dokumentation sollte das generelle Vorgehen im Risikofrüherkennungssystem ersichtlich sein (z. B. Abbildung von Maßnahmen zur Risikoidentifikation,

Risikoanalyse, Risikokommunikation, von allgemeinen Risikorichtlinien, von festgelegten Verantwortlichkeiten sowie Maßnahmen zur Überwachung). Damit wird eine dauerhafte und personenunabhängige Funktionsfähigkeit der getroffenen Maßnahmen sichergestellt, und es ermöglicht dem Vorstand den Nachweis, seiner Verpflichtung gemäß § 91 Abs. 2 AktG nachgekommen zu sein (= Rechenschaftsfunktion) (vgl. IDW PS 340 1999: Ziff. 3.6). Außerdem dient die Dokumentation der Information der Mitarbeiter und ist gleichzeitig Voraussetzung für die Konzeption und Umsetzung eines im gesamten Unternehmen einheitlich institutionalisierten Risikomanagementprozesses (vgl. Diederichs/Form/Reichmann 2004: 196f). Damit entwickelt sich das Risikomanagementhandbuch zu einer Unternehmensrichtlinie. Hinzu kommt, dass die Dokumentation die Grundlage für die Prüfung durch den Wirtschaftsprüfer bildet (= Prüfbarkeitsfunktion) (vgl. Lehner/Schmidt 2000: 268). Eine ausreichende Dokumentation lässt den Prüfer erkennen, dass die eingeleiteten Maßnahmen gemäß § 91 Abs. 2 AktG im Unternehmen kontinuierlich und vollständig umgesetzt wurden.

Eine verbindliche Vorgabe für die Strukturierung des Handbuchs gibt es nicht. Generell sollte das Risikomanagementhandbuch diejenigen Angaben enthalten, anhand derer sich ein sachverständiger Dritter (insbesondere der Abschlussprüfer) in angemessener Zeit ein Bild über die getroffenen Maßnahmen machen kann. Für den inhaltlichen Aufbau bietet sich beispielsweise die aus Anlage 4 ersichtliche Darstellung an.

Wie aus den Ausführungen ersichtlich ist, verfolgt die Wirtschaftsprüferseite eine etwas andere Intention als die betriebswirtschaftliche Forschung hinsichtlich der Anforderungen an ein „Risikomanagementsystem“. Um die Prüfungsfähigkeit des Risikofrüherkennungssystems zu gewährleisten, stellt das IDW insbesondere auf die Risikoverantwortlichen sowie auf eine Dokumentationsfunktion ab (vgl. Bitz 2000a: 234). Damit ist die Wirtschaftsprüfung auch weniger an einer Integration des Risikofrüherkennungssystems im gesamten Unternehmen interessiert, weil das die Prüfung erschweren würde (vgl. Wall 2003: 468). Die Betriebswirtschaftslehre hingegen verbindet gerade mit der Integration erhebliche Vorteile, die sich aus der Einsparung von Kosten, der Vermeidung von Redundanzen sowie der Förderung eines Risikobewusstseins im Unternehmen ergeben, wie schon im Abschnitt 5.1.1. herausgestellt wurde.

#### 6.1.2.2. Unterschiede zum betriebswirtschaftlichen Risikomanagement

In diesem Abschnitt sollen nun die Anforderungen an ein „Risikomanagement“ gemäß IDW PS 340 den betriebswirtschaftlichen Anforderungen gegenübergestellt und auf weitere Unterschiede aufmerksam gemacht werden. Dabei ist zu beachten, dass sich der Prüfungsstandard als Folge der durch das KonTraG neu eingeführten gesetzlichen Verpflichtung gemäß § 317 Abs. 4 HGB entwickelt hat und deshalb auch der Bezug zum KonTraG bestehen bleibt.

Ein grundlegender Unterschied besteht insbesondere im Anwendungsbereich der beiden Konzeptionen, so ist das betriebswirtschaftliche Risikomanagement an alle Unternehmen unabhängig von Größe und Komplexität gerichtet, während sich der Prüfungsstandard an Aktiengesellschaften oder andere Gesellschaften mit vergleichbarer Struktur wendet.

Ein wesentlicher Unterschied liegt vor allem auch in der Verwendung des Begriffs Risiko. Während die betriebswirtschaftliche Seite hauptsächlich auf Risiken und Chancen gerichtet ist, so bezieht sich der IDW PS 340 lediglich auf die negative Ausprägung des Risikos. Die Perspektive des externen Prüfers ist damit vorrangig auf die Verlustgefahren gerichtet. Betriebswirtschaftlich gesehen, kommt den Chancen eine größere Bedeutung zu, da diese das Erfolgspotenzial für ein Unternehmen darstellen und das größte unternehmerische Risiko im Versäumnis von Chancen besteht (vgl. Horvath 2003b: 217). Mit der negativen Sichtweise des KonTraG und des IDW PS 340 entsteht die Gefahr, dass die Risikovermeidung in den Unternehmen im Vordergrund stehen könnte und damit die betriebswirtschaftlichen Chancen nicht mehr wahrgenommen werden. Die Folge ist eine unzureichende Weiterentwicklung der Erfolgspotenziale und eine fehlerhafte Ausrichtung der Unternehmensstrategie. Erste Ansätze in neuen Gesetzesvorlagen insbesondere im BilReG zeigen jedoch, dass vermehrt eine Ausrichtung auf Chancen vom Gesetzgeber beabsichtigt wird, so dass eine Annäherung an die betriebswirtschaftlichen Anforderungen stattfindet.

Ein weiterer Unterschied ist im Hinblick auf das Ausmaß der Risiken erkennbar. Dem betriebswirtschaftlichen Risikomanagement ist eine von vornherein gegebene Beschränkung auf bestimmte Risikoausmaße fremd, während sich die Ausführungen gemäß KonTraG und IDW nur auf wesentliche und bestandsgefährdende Risiken beziehen.

Hinzu kommt, dass die Risikosteuerung als Bestandteil des betriebswirtschaftlichen Risikomanagements nicht in den Pflichtumfang der einzurichtenden Maßnahmen gemäß KonTraG und IDW gehört (vgl. Wall 2003: 460), sich aber aus der Leitungsaufgabe und der Sorgfaltspflicht des Vorstandes ergibt.

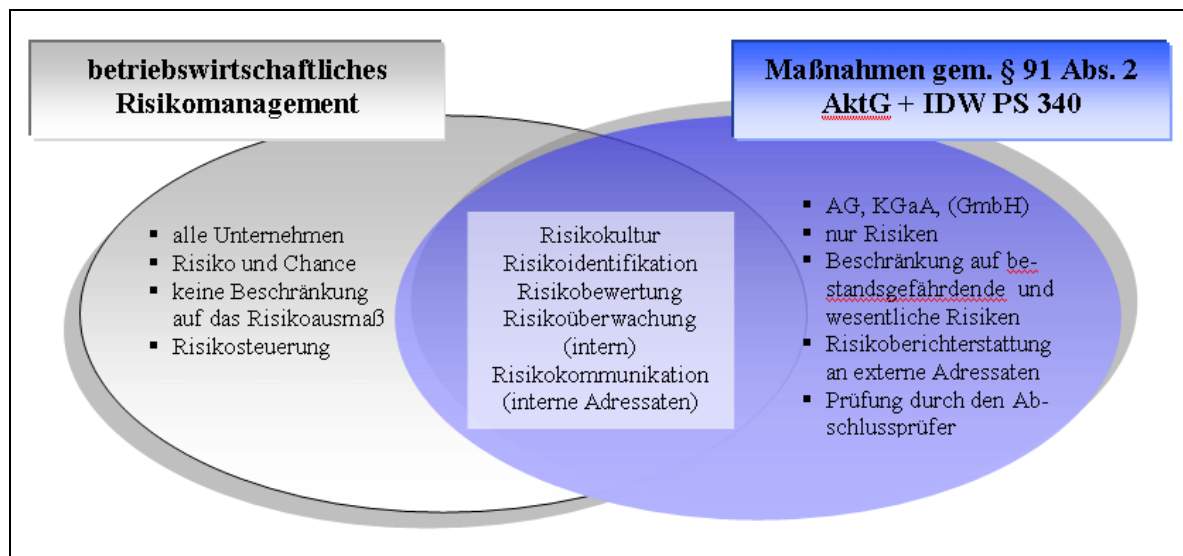
Hingegen spielen Akteure wie Abschlussprüfer sowie eine von der Rechtsform abhängige Differenzierung zwischen Vorstand und Aufsichtsrat wiederum im klassischen betriebswirtschaftlichen Risikomanagement keine Rolle, da sich die grundlegenden Anforderungen an alle Unternehmen richten sollen.

Es besteht wohl auch kein Zweifel daran, dass der Risikoberichterstattung an die unternehmensexternen Adressaten des Kapitalmarktes keine entsprechende Funktion im traditionellen Verständnis des betriebswirtschaftlichen Risikomanagement gegenübersteht. Dort ist die Berichterstattung/Kommunikation von Risiken zwar eine immer wieder hervorgehobene Notwendigkeit, allerdings stehen dabei die unternehmensinternen Adressaten im Mittelpunkt. Mit dem KonTraG gelangt damit das bislang der eher unternehmensinternen

Sphäre der Unternehmensführung zugeordnete Risikomanagement explizit in das Blickfeld von Unternehmensexternen (vgl. Wall 2002: 2).

Insgesamt kann festgehalten werden, dass die Vorschriften des KonTraG und des IDW PS 340 generell im Einklang mit dem Verständnis des betriebswirtschaftlichen Risikomanagements stehen. Dies äußert sich vor allem in dem Ziel der Förderung einer Risikokultur im gesamten Unternehmen. Weitere Überschneidungen zwischen den gesetzlichen Anforderungen, den Anforderungen der Wirtschaftsprüfer und denen des betriebswirtschaftlichen Risikomanagements sind aus Abbildung 18 zu entnehmen. Zur Schnittmenge gehören vor allem die Funktionen, die der Risikofrüherkennung, -bewertung und -überwachung zuzuordnen sind.

*Abbildung 18: Unterschiede zwischen § 91 Abs. 2 AktG, IDW PS 340 und dem betriebswirtschaftlichem Risikomanagement*



Quelle: In Anlehnung an Wall (2002: 14).

Für ein Unternehmen, das über ein betriebswirtschaftliches Risikomanagement verfügt, dürften sich, abgesehen von der Erstellung einer für die Prüfung geeigneten Dokumentation und der externen Berichterstattung, aus den gesetzlich geforderten Regelungen sowie den Anforderungen des IDW PS 340 kaum Probleme ergeben.

Die angesprochenen Pflichten des Vorstands stellen in betriebswirtschaftlicher Hinsicht nicht etwas wirklich Neues dar. Die in § 91 Abs. 2 AktG aufgestellte Forderung erscheint betriebswirtschaftlich als Selbstverständlichkeit und gehört rechtlich gesehen eigentlich zu den Pflichten eines Vorstandes. Neu ist jedoch die Konkretisierung im Aktiengesetz, die damit einen gesetzlich definierten „Mindest-Pflichtenrahmen“ (vgl. Zimmer/Sonneborn 2001: 55) für eine Risikofrüherkennung des Vorstandes vorgibt.

Die Verpflichtung zur Einrichtung und zum Betrieb eines nach § 91 Abs.2 AktG entsprechenden Risikofrüherkennungssystems sollte damit von der Unternehmenspraxis nicht in erster Linie als Kosten verursachende Auflage des Gesetzgebers verstanden werden, sondern als Anstoß, die bislang eventuell vorhandenen Ansätze zu einem geschlossenen, effektiven Risikomanagement auszubauen, um den Fortbestand des Unternehmens zu sichern.

## 6.2. Internationale Anforderungen

Während man in Deutschland mit dem KonTraG in Form einer gesetzlichen Vorschrift zur Risikofrüherkennung und -überwachung auf die zahlreichen Unternehmensskandale reagierte, dominieren international rechtlich unverbindliche Verhaltenskodizes („Codes of Best Practise“), die eine ordnungsgemäße Unternehmensführung sicherstellen sollen (vgl. Brebeck/Hermann 1997: 381). Eine Vorbildfunktion für die verschiedenen nationalen Regelwerke hat dabei der bereits 1992 in den USA veröffentlichte **COSO Report „Internal Control – Integrated Framework“** erlangt. COSO stellt Grundlagen eines effektiven Kontrollsystems für eine verbesserte Unternehmensführung („Corporate Governance“) dar und berücksichtigt als erste und umfassende Methode auch eine Risikofrüherkennung und -überwachung im Unternehmen (vgl. Romeike 2003b: 66). Nachdem COSO 1992 entwickelt wurde, hat die IFAC<sup>10</sup> begonnen, das Rahmenwerk in ihre Prüfungsstandards aufzunehmen (ISA 400,<sup>11</sup> ISA 315 und 330).<sup>12</sup> Parallel dazu wurde es in die U.S. Wirtschaftsprüfungsstandards integriert (AU 312, AU 319).<sup>13</sup> Inzwischen haben über 63 % der US-börsennotierten Unternehmen COSO als führendes Rahmenwerk implementiert. Sogar der Basler Ausschuss (1998: 10ff) empfiehlt den Banken eine Ausrichtung an diesem Report. Auch in Deutschland bildet COSO die Grundlage für einen Prüfungsstandard (IDW PS 260 - Das interne Kontrollsystem im Rahmen der Abschlussprüfung) (vgl. IDW PS 260 2001: 821ff). Da sich damit viele internationale Prüfungsstandards grundlegend an diesem Rahmenwerk orientieren (vgl. Eichler/Bungartz 2004: 108), soll COSO im Abschnitt 6.2.1. genauer untersucht werden.

Auf Grund der spektakulären Bilanzskandale in den USA im Jahre 2001

<sup>10</sup> Vgl. Mertin/Schmidt (2001: 318). Die IFAC ist ein globaler Berufsverband der Wirtschaftsprüfer. Sie zählt 159 Berufsverbände wie den IDW zu ihren Mitgliedern. Im öffentlichen Interesse vertritt die IFAC den Berufszweig der Wirtschaftsprüfer und erlässt die international anerkannten International Standards on Auditing (ISA).

<sup>11</sup> Vgl. Mertin/Schmidt 2001: 326; ISA 400 (Risk Assessment and Control).

<sup>12</sup> Vgl. Menzies 2004: 85; ISA 315 (Understanding the Entity and its Environment and Assessing the Risks of Material Misstatement), ISA 330 (The Auditor`s Procedures in Response to Assessed Risks).

<sup>13</sup> Vgl. Jacob 2001: 241, AU 312 (Audit Risk and Materiality in Conducting an Audit), AU 319 (Consideration of Internal Control in an Financial Statement).



(Enron) und im Jahre 2002 (Worldcom) (vgl. Schwarz/Holland 2002: 1661) gewann COSO erneut große Bedeutung. Der amerikanische Gesetzgeber sah sich nun dringend gezwungen auf die weiteren Unternehmensschieflagen zu reagieren und verabschiedete in einem außerordentlich kurzen Gesetzgebungsverfahren am 30. Juli 2002 den so genannten **Sarbanes-Oxley-Act** (vgl. Buderath 2004: 40). Ziel des Gesetzes war es, insbesondere das Vertrauen der Anleger wiederherzustellen und sie vor betrügerischen Handlungen in der Rechnungslegung zu schützen. Die Verabschiedung des Sarbanes-Oxley-Act in den USA bildet damit einen weiteren wichtigen Baustein in den weltweit erkennbaren Bestrebungen, Corporate-Governance-Strukturen zu stärken (vgl. Buderath 2004: 39). Mit dem Gesetz soll der Wahrheitsgehalt der Rechnungslegungsinformationen und die Unternehmenstransparenz sichergestellt werden, in dem die Chief Executive Officer (CEO) und Chief Financial Officer (CFO) künftig die Richtigkeit und Vollständigkeit der Finanzberichterstattung durch ihre Unterschrift beider müssen. Nach dem Gesetz muss das Management nun auch nachweisen, ein angemessenes und wirksames Kontrollsystem für die ordnungsgemäße Finanzberichterstattung eingerichtet zu haben (Internal Control over Financial Reporting), das von einem unabhängigen Abschlussprüfer im Rahmen der Jahresabschlussprüfung testiert werden muss (vgl. Lanfermann/Maul 2002: 1727).

Um die Unabhängigkeit des Wirtschaftsprüfers vom geprüften Unternehmen zu gewährleisten, verlangt der Sarbanes-Oxley Act unter anderem auch eine stärkere Trennung des Prüfungsgeschäfts vom Beratungsgeschäft. Des Weiteren forderte der Sarbanes-Oxley-Act die Einrichtung einer neuen Aufsichtsbehörde (PCAOB = Public Company Accounting Oversight Board), bei der sich alle Wirtschaftsprüfer registrieren lassen müssen, um die Umsetzung einheitlicher Prüfungsstandards und die Überwachung der Wirtschaftsprüfer zu gewährleisten (vgl. Ferlings/Lanfermann 2002: 2118). Diese neue Aufsichtsbehörde wird wiederum von der „Securities and Exchange Commission“ (SEC), der staatlichen Wertpapieraufsichtsbehörde der USA, überwacht (vgl. Lanfermann/Maul 2002: 1725).

Damit das Management den neuen Anforderungen gerecht werden kann und das interne Kontrollsystem für die richtige und wahrheitsgemäße Finanzberichterstattung auch wirksam ist, hat die SEC das COSO-Rahmenwerk als Standard und „Best-Practice“ empfohlen. Diese Tatsache unterstreicht noch einmal die Bedeutung und Anerkennung von COSO.

Da der Sarbanes-Oxley-Act sämtliche bei der SEC registrierte Unternehmen betrifft, weist das Gesetz auch Auswirkungen auf viele deutsche Unternehmen aus, die bei der SEC registriert sind. Dies gilt auch für Tochtergesellschaften solcher Unternehmen (vgl. Lanfermann/Maul 2002: 1725). Aus einer Studie von Ernst & Young geht hervor, dass dadurch ca. 300 deutsche Unternehmen dem Sarbanes-Oxley-Act unterliegen, die demzufolge COSO implementieren

sollten (vgl. Buderath 2004: 40). Da in Deutschland bereits seit 1998 durch das KonTraG für Aktiengesellschaften eine Pflicht zur Einführung eines Risikofrüherkennungs- und Überwachungssystems besteht, ergeben sich daraus sicherlich Überschneidungen mit der Einführung von COSO in diesen Unternehmen, da COSO ebenfalls Maßnahmen zur Risikofrüherkennung und Überwachung beinhaltet.

Da COSO I nun seit längerem keine Ergänzung und Änderung fand und sich die Forderung nach einer stärkeren Risikoausrichtung und -orientierung im Rahmenwerk erhöhte, wurde COSO I um ein **Enterprise Risk Management** ergänzt, auf das es im Abschnitt 6.2.2. näher einzugehen gilt.

### 6.2.1. COSO Internal Control – Integrated Framework

Ziel dieses Abschnitts soll es nun sein, COSO als Rahmenwerk vorzustellen. Dabei gilt es zunächst Entwicklung, Aufbau und Ziele von COSO zu untersuchen.

Das Committee of Sponsoring Organizations of the Treadway Commission (COSO) ist eine im Jahre 1985 gegründete Initiative privatwirtschaftlicher amerikanischer Wirtschaftsinstitute (vgl. COSO 1992: 96), die das Ziel verfolgt, Ursachen für betrügerische Handlungen bei der Finanzberichterstattung aufzudecken.<sup>14</sup> Die sich damals über drei Jahre erstreckenden Untersuchungen, an denen Hunderte von Fachleuten mitarbeiteten, endeten 1992 mit dem COSO-Report, der als Ursachenfaktor unwirksame interne Kontrollsysteme identifizierte (vgl. Menzies 2004: 76). Da ein internes Kontrollsystem ein wichtiger Bestandteil guter und verantwortungsvoller Unternehmensführung („Corporate Governance“) ist, und es bis dahin in den USA kein allgemein akzeptiertes Verständnis von Internal Control gab, bestand das Ziel darin, mit COSO Internal Control – Integrated Framework einen einheitlichen Bezugsrahmen zu schaffen, der viele bis dahin gewonnene wissenschaftliche und praktische Erkenntnisse über interne Kontrollsysteme in sich vereinen sollte (vgl. Neubeck 2003: 222). So wurde in Zusammenarbeit mit Coopers und Lybrand, Rechtsvorgänger von PwC, eine einheitliche Definition des internen Kontrollsystems entwickelt, die sich an alle Unternehmen unabhängig von Größe, Rechtsform und Kapitalmarktzugang richtet (vgl. Kajüter 2003: 50f).

#### 6.2.1.1. Aufbau und Ziele von COSO

Der COSO-Report besteht aus vier Teilen, wobei der erste Teil des Berichts eine Zusammenfassung (Executive Summary) über die Ergebnisse der Untersuchungen beinhaltet. Im zweiten Teil (Framework) wird ein internes Kontrollsystem zum einen definiert und zum anderen werden seine Komponenten näher beschrieben und Kriterien zur Systemeinschätzung dargestellt. Der dritte

---

<sup>14</sup> Vgl. [www.coso.org](http://www.coso.org), 24.06.2004.

Teil gibt den Unternehmen Hinweise zur externen Berichterstattung (Reporting to External Parties) und im abschließenden vierten Teil werden Werkzeuge dargelegt, die eine Bewertung des internen Kontrollsystems ermöglichen sollen.

Im Rahmen der Ausführungen dieses Abschnitts soll vor allem der zweite Teil des COSO-Reports im Mittelpunkt der Betrachtungen stehen, da hier die Anforderungen an ein internes Kontrollsystem im Detail erläutert werden.

COSO definiert das interne Kontrollsystem als einen kontinuierlichen **Prozess** (vgl. COSO 1992: 14), der von Aufsichtsgremien, Management und Mitarbeitern verantwortungsvoll ausgeführt werden soll, um nachstehende Ziele zu erreichen:

- Effektivität und Effizienz von betrieblichen Abläufen sicherzustellen (**Operations**),
- die Ordnungsmäßigkeit und Verlässlichkeit der Finanzberichterstattung zu gewährleisten (**Financial Reporting**),
- sowie die Einhaltung von Gesetzen und Vorschriften zu überwachen (**Compliance**) (vgl. COSO 1992: 13; Heese 2003: 225).

**Alle Risiken**, die das Unternehmen an der Erreichung dieser Ziele hindern, sollen durch **interne Kontrollen** wirksam vermindert werden (vgl. Menzies 2004: 77). Um dies zu ermöglichen, empfiehlt COSO fünf miteinander zu verknüpfende Komponenten, die in die bestehenden Geschäftsprozesse zu integrieren sind. Die Integration hat den Vorteil, dass sie zusätzliche Kosten und Aufwand vermeidet und alle Mitarbeiter im Unternehmen am internen Kontrollsystem teilhaben lässt (vgl. COSO 1992: 15).

#### 6.2.1.2. Komponenten von COSO

Die einzelnen Komponenten sollen im Folgenden beschrieben werden. Dabei ist zu beachten, dass die Ausgestaltung jeder Komponente unternehmensspezifisch zu erfolgen hat (vgl. COSO 1992: 18).

Abbildung 19: COSO-Modell



Quelle: COSO Internal Control – Integrated Framework (1992: 19).

Das Modell von COSO entspricht einem Würfel. Die drei Zielkategorien beziehen sich dabei auf alle fünf Komponenten. Alle Zielkategorien und Komponenten sind wiederum in allen organisatorischen Einheiten des Unternehmens vorhanden.

#### 6.2.1.2.1. Control Environment (Steuerungsumfeld, Kontrollumfeld)

Das Steuerungsumfeld bildet das Fundament für alle weiteren Komponenten des internen Kontrollsystems. Hier werden ethische Werte, die Unternehmensphilosophie, die Unternehmensstrategie/-ziele, die Risikoeinstellung des Unternehmens und der Führungsstil festgelegt und an alle Mitarbeiter kommuniziert (vgl. COSO 1992: 23ff). Außerdem werden in dieser Phase die Kontrollaktivitäten zur Erreichung der Unternehmensziele den Verantwortlichen

vor allem im operativen Bereich übertragen, da hier eine besondere Nähe zum Tagesgeschäft besteht (vgl. COSO 1992: 28). Dafür ist es notwendig, den Mitarbeitern umfangreiche Schulungsmaßnahmen zur Verfügung zu stellen. Damit soll das Bewusstsein für interne Kontrollen bei allen Mitarbeitern gestärkt werden. Doch nicht nur die Kontrollaktivitäten der Mitarbeiter, sondern auch die Überwachungsarbeit der Aufsichtsgremien ist bedeutend für die Funktionsfähigkeit eines internen Kontrollsystems. Ein mangelhaftes Steuerungsumfeld kann letztendlich die Mitarbeiter zu illegalen Handlungen (Manipulation von finanziellen Daten) ermutigen und in der Folge zu einem Imageverlust oder zu einem finanziellen Verlust für das Unternehmen führen (vgl. COSO 1992: 30).

#### 6.2.1.2.2. Risk Assessment (Risikobeurteilung)

Durch die Integration von Kontrollen in den Geschäftsprozess soll sichergestellt werden, dass alle Risiken (Hindernisse) identifiziert und bewertet werden, die das Unternehmen an der Erreichung seiner Ziele (Operations, Financial Reporting, Compliance) und Unterziele hindern. Zur Identifikation der Risiken empfiehlt COSO, alle Unternehmensbereiche auf negative externe und interne Einflüsse hin zu untersuchen. Dies ist besonders wichtig, da sich Risiken negativ auf den Unternehmensfortbestand, den Wettbewerb, die Produkte, die Finanzen und das Image des Unternehmens auswirken können (vgl. COSO 1992: 33). Als externe Risiken nennt COSO beispielhaft technologische Entwicklungen, Veränderung der Kundenwünsche, Erhöhung des Wettbewerbs, verschärfte gesetzliche Rahmenbedingungen sowie Naturkatastrophen. Zu den internen Risiken gehören beispielsweise ein schlechtes Informationssystem, unmotiviertes oder unqualifiziertes Personal und ein häufiger Wechsel des Managements (vgl. COSO 1992: 40f). Als zusätzliche Informationsquellen zur Identifikation von Risiken sollen insbesondere Kunden, Mitarbeiter, Medien, Lieferanten, Aktionäre und Banken genutzt werden. Darüber hinaus ist es wichtig, nicht an vordefinierten und bereits bekannten Risiken aus der Vergangenheit anzuknüpfen, sondern alle Möglichkeiten zu betrachten aus denen zukünftig Risiken hervorgehen können. Dafür ist es notwendig ein Frühwarnsystem im Unternehmen zu implementieren, um rechtzeitig Gegenmaßnahmen für auftretende Risiken einleiten zu können (vgl. COSO 1992: 45f). Die Risikoidentifikation sollte dabei nicht als einmaliger Prozess verstanden werden, sondern aufgrund der Dynamik von Veränderungen in Umwelt und Unternehmen mehrmals im Jahr stattfinden. Zu beachten ist außerdem, dass nur auch für das Unternehmen relevante Risiken betrachtet werden sollen (vgl. COSO 1992: 42).

Um die Bedeutung der identifizierten Risiken für das Unternehmen messen zu können, gilt es die Risiken einer Bewertung zu unterziehen. Dabei werden Eintrittswahrscheinlichkeit und Auswirkung eines Risikos ermittelt, um im Anschluss unter Kosten-Nutzen-Überlegungen Risiken effizient managen zu

können.

Schließlich hat das Management zu entscheiden, bis zu welcher Höhe Risiken einzugehen sind, um die Unternehmensziele zu erreichen. Im Rahmenwerk wird unter anderem auch darauf hingewiesen, dass eine Unternehmenstätigkeit immer mit Risiken verbunden ist und Risiken nicht vollständig vermieden werden können, sondern es nur möglich ist, Risiken in ihrem Ausmaß und ihrer Eintrittswahrscheinlichkeit zu vermindern (vgl. COSO 1992: 33). Die dafür zu ergreifenden Maßnahmen überlässt COSO grundsätzlich dem Ermessen des Managements und erwähnt nur eventuell mögliche Handlungen wie beispielsweise die Begrenzung des Schadensausmaßes der Risiken durch Versicherungen oder das Hedgen von Risiken. Generell stellt die Reaktion auf Risiken jedoch keinen Bestandteil des internen Kontrollsystems dar. Das System selbst bildet aber die Grundlage für Managemententscheidungen über den Umgang mit Risiken (vgl. COSO 1992: 43).

#### 6.2.1.2.3. Control Activities (Kontrollaktivitäten)

Diese Komponente des Internen Kontrollsystems soll sicherstellen, dass alle Managemententscheidungen eingehalten und Maßnahmen korrekt ausgeführt werden (vgl. COSO 1992: 49). Um dies zu überwachen, müssen im Unternehmen verschiedene Kontrollaktivitäten eingeführt werden. Sie sind zunächst genau zu definieren und in ihrer Durchführung zu beschreiben. Unter anderem gilt es sich auch zu vergewissern, dass rechtzeitig Maßnahmen zur Risikosteuerung ausgeführt wurden, um die Zielerreichung nicht zu gefährden (vgl. COSO 1992: 51f). Diese Kontrollen werden dabei in allen Bereichen und Unternehmensebenen durchgeführt und beziehen sich unter anderem auch auf die Überprüfung von Konten hinsichtlich Ordnungsmäßigkeit der Rechnungslegung oder die Sicherheitsprüfung von IT-Systemen und Software, sowie die Überwachung von Produktionsprozessen und die Einhaltung von Autoritäten (vgl. COSO 1992: 52f).

#### 6.2.1.2.4. Information & Communication (Information und Kommunikation)

Information und Kommunikation bilden die Grundlage für die Entscheidungsfindung des Managements. Ein internes Kontrollsystem muss Informationen nicht nur identifizieren, sondern auch rechtzeitig, übersichtlich und korrekt an den richtigen Entscheidungsträger kommunizieren (vgl. COSO 1992: 62), um frühzeitig Gegenmaßnahmen einleiten zu können. Vor allem muss die Unternehmensleitung über den Stand der Erreichung der unter 6.2.1.1. definierten Ziele unterrichtet werden (vgl. COSO 1992: 59). Umgekehrt ist auch eine laufende Informationsübermittlung (Strategie, Philosophie, Erwartungshaltung) der Unternehmensführung an die Mitarbeiter im Unternehmen wichtig. Auch die Informationsversorgung der Aufsichtsgremien im Unternehmen sollte gewährleistet sein und die Aufsichtsgremien wiederum sollten kommunizieren,

welche Informationen sie für die Ausführung ihrer Überwachungstätigkeit benötigen. Voraussetzung dafür sind funktionierende Informations- und Kommunikationswege im Unternehmen (vgl. COSO 1992: 63). Die Informationen sollen sich dabei nicht nur auf interne Daten beschränken, sondern auch externe Bedingungen und Ereignisse in die Berichterstattung einbeziehen (vgl. COSO 1992: 65).

In diese Komponente des internen Kontrollsystems gehört auch die Kommunikation mit Kunden, Lieferanten und Aktionären, um wichtige Informationen schnell zu erhalten und auf veränderte Bedürfnisse reagieren zu können. Auch in der Produktion sollten moderne Informationssysteme eingesetzt werden, die beispielsweise über die Materialbeschaffenheit von Produkten informieren können (vgl. COSO 1992: 61).

#### 6.2.1.2.5. Monitoring (Überwachung)

Die letzte Komponente eines internen Kontrollsystems beinhaltet die Überwachung der Qualität und Leitung des internen Kontrollsystems selbst. Dies ist erforderlich, da sich Unternehmen und Umwelt in einem ständigen Wandel befinden und permanente Änderungen im internen Kontrollsystem notwendig erscheinen. Erfolgt keine ständige Anpassung des Systems, so kann dies dazu führen, dass Risiken nicht rechtzeitig erkannt werden (vgl. COSO 1992: 69). Die Überwachung soll gewährleisten, dass das interne Kontrollsystem weiterhin effektiv arbeitet.

Zur besseren Überwachung empfiehlt COSO das interne Kontrollsystem zu dokumentieren. COSO leitet die Effektivität des Systems jedoch nicht von der Dokumentation ab (vgl. COSO 1992: 73).

Die Überwachung des internen Kontrollsystems erfolgt durch prozessintegrierte Maßnahmen wie sie auch schon in der dritten Komponente beschrieben wurden. Träger dieser Aufgabe ist oftmals das Controlling (vgl. COSO 1992: 50). Gegebenfalls wird eine prozessübergreifende Überwachung eingesetzt, die meistens von der internen Revision im Unternehmen durchgeführt wird (vgl. COSO 1992: 71f).

Zu beachten ist, dass eine öffentliche Berichterstattung weder eine Komponente noch ein Kriterium für ein internes Kontrollsystem nach COSO darstellt, weil die Effektivität des internen Kontrollsystems nicht von ihr abhängt. Die Grundsätze von COSO befürworten und unterstützen die Berichterstattung (**finanzielle Berichterstattung**) jedoch stark. In den USA ist COSO der verbreitetste Standard für die Einrichtung von Internal Controls over Financial Reporting in Zusammenhang mit dem Sarbanes-Oxley-Act (vgl. Heese 2003: 226).

Letztendlich bestimmen die Größe des Unternehmens, die bestehende Unternehmenskultur sowie länderspezifische Besonderheiten maßgeblich, in welchem Umfang die Komponenten des COSO Modells anzuwenden sind. In jedem Fall sollte das Management jedoch sicherstellen, dass die einzelnen

Komponenten im Unternehmen hinreichend Berücksichtigung finden, um die Effektivität des internen Kontrollsystems zu gewährleisten. Die Elemente müssen für alle betrieblichen Einheiten und vor allem konzernweit wirkungsvoll eingesetzt werden (vgl. Heese 2003: 226). Hinzu kommt, dass die Ausgestaltung des Systems immer unter Kosten-Nutzen-Überlegungen erfolgen sollte (vgl. COSO 1992: 81).

Im Rahmenwerk wird jedoch mehrmals betont, dass ein gut implementiertes Kontrollsystem nach COSO keinen Erfolg und keinen Fortbestand des Unternehmens garantieren kann. Die Erwartungen an ein solches System müssen realistisch bleiben, zumal Fehlentscheidungen von handelnden Personen nicht vollständig auszuschließen sind (vgl. COSO 1992: 80).

#### 6.2.1.3. Vergleich zum betriebswirtschaftlichen Risikomanagement

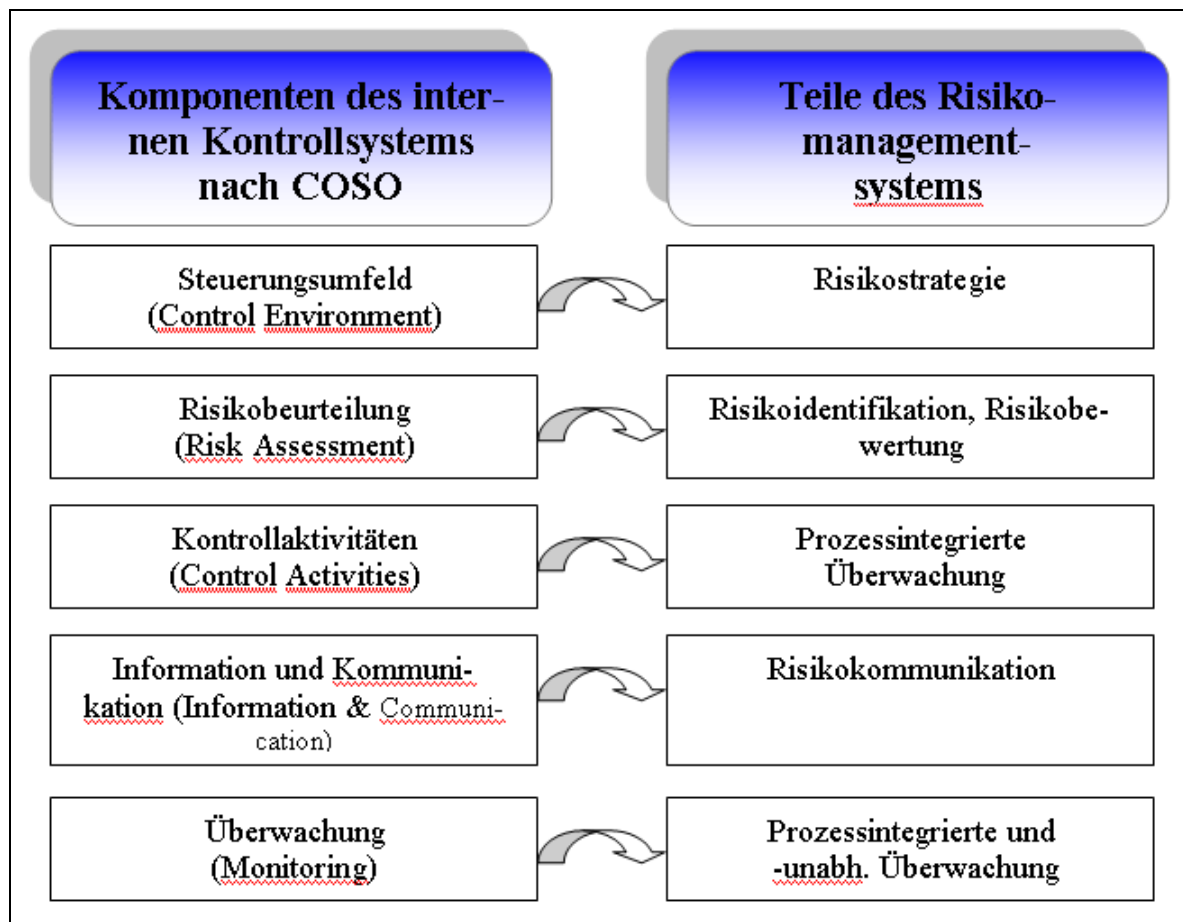
Nachdem nun die grundlegenden Inhalte von COSO vorgestellt wurden, soll in diesem Abschnitt das Rahmenwerk mit den betriebswirtschaftlichen Anforderungen an ein Risikomanagement verglichen werden. Obwohl bei einer Betrachtung der Zielkategorien deutlich wird, dass mit COSO im Vergleich zum betriebswirtschaftlichen Risikomanagement zunächst andere Hauptzielrichtungen verfolgt werden, bestehen jedoch bei den einzelnen Komponenten viele Gemeinsamkeiten.

Nach einer näheren Untersuchung ist zu erkennen, dass Teile eines Risikomanagementsystems Bestandteile des internen Kontrollsystems nach COSO sind (vgl. Buderath 2003: 220).

So sind die fünf miteinander verknüpften Komponenten des internen Kontrollsystems grundsätzlich mit Teilen des dieser Arbeit zu Grunde liegenden Risikomanagementsystems vergleichbar, wie auch aus nachstehender Abbildung ersichtlich ist.



Abbildung 20: Vergleich der Komponenten von COSO mit Elementen des Risikomanagements



Quelle: Eigene Darstellung.

Das Steuerungsumfeld stimmt grundsätzlich mit der Risikostrategie überein, die den Ausgangspunkt für alle Prozesselemente des Risikomanagementsystems bildet.

Auch die Komponente der Risikobeurteilung weist eine hohe Ähnlichkeit mit denen in den Abschnitten 5.1.2. Risikoidentifikation und 5.1.3. Risikobewertung dargestellten Prozess-elementen eines betriebswirtschaftlichen Risikomanagements auf. Unterschiede bestehen jedoch in der fehlenden Berücksichtigung von Chancen im COSO-Rahmenwerk, sowie der Vernachlässigung möglicher Interdependenzen zwischen Risiken. Eine Beschränkung auf ein bestimmtes Risikoausmaß findet im Gegensatz zum IDW PS 340 nicht statt. Die Risikosteuerung wird wiederum der Leitungs- und Sorgfaltspflicht der Unternehmensleitung überlassen und ist nicht Bestandteil des COSO-Rahmenwerkes.

Dagegen gehen die Komponenten „Kontrollaktivitäten“, „Überwachung“, „Information und Kommunikation“ über die Bestandteile des Risikomanagements hinaus. Während die entsprechenden Komponenten im Risikomanagement

mentprozess grundsätzlich „risikomanagementbezogen“ sind, betreffen die Komponenten des COSO-Reports sämtliche Unternehmensaktivitäten. Damit stellt COSO zusätzliche Anforderungen an ein internes Kontrollsystem, auf die im Einzelnen nicht weiter eingegangen werden soll. Letztendlich kann festgehalten werden, dass ein Risikofrüherkennungs- und Überwachungssystem ein Teil eines umfassenden internen Kontrollsystems darstellt. Somit gibt es in den USA bereits seit 1992 einen Orientierungsrahmen für die Implementierung eines Risikofrüherkennungssystems.

Obgleich COSO umfangreichere Angaben als das KonTraG und der IDW PS 340 enthält, gibt das Rahmenwerk auch nur allgemeine Vorgaben zur Ausgestaltung der Systeme vor, so dass die Unternehmen in dieser Hinsicht über Gestaltungsspielräume verfügen. Ein wesentlicher Unterschied besteht jedoch im Anwendungsbereich. So richtet sich COSO ebenso wie das betriebswirtschaftliche Risikomanagement an alle Unternehmen unabhängig von Größe, Rechtsform und Kapitalmarktorientierung (vgl. COSO 1992: 6ff).

### 6.2.2. COSO - Enterprise Risk Management

Fast elf Jahre nach der Veröffentlichung von COSO I (Internal Control – Integrated Framework) wurde auf Grund verstärkter Corporate Governance Diskussionen zunehmend der Bedarf an einem Rahmenwerk für ein ganzheitliches Risikomanagementsystem erkannt. Obwohl COSO I bereits Teile von Risikofrüherkennung und -überwachung beinhaltet, bestand die Notwendigkeit detaillierter auf den Umgang mit Risiken einzugehen. Begründet wurde diese Entscheidung vor allem mit der steigenden Anzahl von Risiken, denen Unternehmen gegenüberstehen und aufgrund festgestellter Mängel bei bereits vorhandenen Risikomanagementsystemen in Unternehmen. Zudem wurde schon seit längerem kritisiert, dass seit dem Jahre 1992 keine Anpassung der COSO-Kriterien erfolgt ist und die Risikoproblematik nicht ausreichend Beachtung fand (vgl. Neubeck 2003: 224).

Da das Thema „Risikomanagement“ bereits in zahlreichen Literaturveröffentlichungen aufgegriffen wurde, es hier aber bisher keine einheitliche Vorgehensweise und keine einheitliche Struktur gibt, bestand mit der Entwicklung von COSO II (Enterprise Risk Management) das Ziel darin, einen Standard zu schaffen, an dem sich die Unternehmen bei der Implementierung eines Risikomanagementsystems halten oder ihr bereits vorhandenes Risikomanagementsystem auf Effektivität überprüfen können (vgl. COSO 2004: 38).

Für das Rahmenwerk wurde ein Budget von 10.000 Stunden veranschlagt (vgl. Neubeck 2003: 224) und an seiner Entwicklung haben sämtliche Personen mit Fachkompetenz aus Wirtschaft und Forschung mitgewirkt. So vereint COSO II sämtliche betriebswirtschaftlichen Erkenntnisse und praktische Erfahrungen in sich (vgl. COSO 2004: 7). Geleitet wurde das Vorhaben wie bei COSO I ebenfalls von PwC (vgl. COSO 2004: Appendix A: 1). Am 15. Juli

2003 wurde das Konzept veröffentlicht und stand bis zum 14. Oktober 2003 für öffentliche Kommentare und Ergänzungsvorschläge zur Verfügung (vgl. Eichler/Bungartz 2004: 108). Mittlerweile wurde COSO II am 29. September 2004 endgültig verabschiedet. Wie COSO I bezieht sich auch COSO II auf alle Unternehmen unabhängig von Größe und Branche (vgl. COSO 2004: 22).

#### 6.2.2.1. Aufbau und Ziele von ERM

Das ERM schließt grundlegend das COSO Rahmenwerk (COSO I) mit ein und ergänzt dieses um ein unternehmensweites Risikomanagement (vgl. COSO 2003: 17). Das bedeutet, dass nicht nur Risikofrüherkennung, sondern auch deren aktive Steuerung und Bewältigung stärker in den Vordergrund rücken (vgl. Heese 2003: 228). Mit Hilfe des ERM sollen Unternehmen Risiken effizienter managen können und dadurch Shareholder Value schaffen. Das ERM-Rahmenwerk stellt dabei eindeutig heraus, dass nicht eine Risikovermeidung angestrebt wird, da sonst auch auf unternehmerische Chancen verzichtet werden muss. Infolgedessen, dass das ERM-Konzept für alle Unternehmen als Basis gelten soll, wurde der Begriff „Enterprise Risk Management“ sehr weit definiert. So ist ERM, „(..) der vom Aufsichtsrat, der Unternehmensleitung, dem operativen Management und den Mitarbeitern umzusetzende **Prozess** zur Strategieformulierung, zur unternehmensweiten Identifizierung wesentlicher Chancen und Risiken und zum Management von Risiken unter Berücksichtigung der Risikobereitschaft des Unternehmens, um das Erreichen der Unternehmensziele zu gewährleisten“ (Eichler/Bungartz 2004: 108; COSO 2004: 6).

Dabei werden durch ERM folgende Unternehmensziele definiert:

- Bestimmung und Unterstützung der Unternehmensstrategie durch die Vorgabe von Unternehmenszielen auf höchster Ebene (**Strategic**),
- Gewährleistung der Effektivität und Effizienz der Geschäftsprozesse (**Operations**)
- Sicherstellung der Ordnungsmäßigkeit und Verlässlichkeit der internen und externen Berichterstattung, auch nicht-finanzieller Daten (**Reporting**)
- Einhaltung relevanter Gesetze und Vorschriften (**Compliance**) (COSO 2003: 11).

Vergleicht man die Ziele mit COSO I, so sind sie überwiegend identisch. Beim ERM erfolgt lediglich eine stärkere Ausrichtung an der Unternehmensstrategie und die Ordnungsmäßigkeit und Verlässlichkeit der finanziellen Berichterstattung wurde auf alle internen und externen Berichte des Unternehmens ausgeweitet.

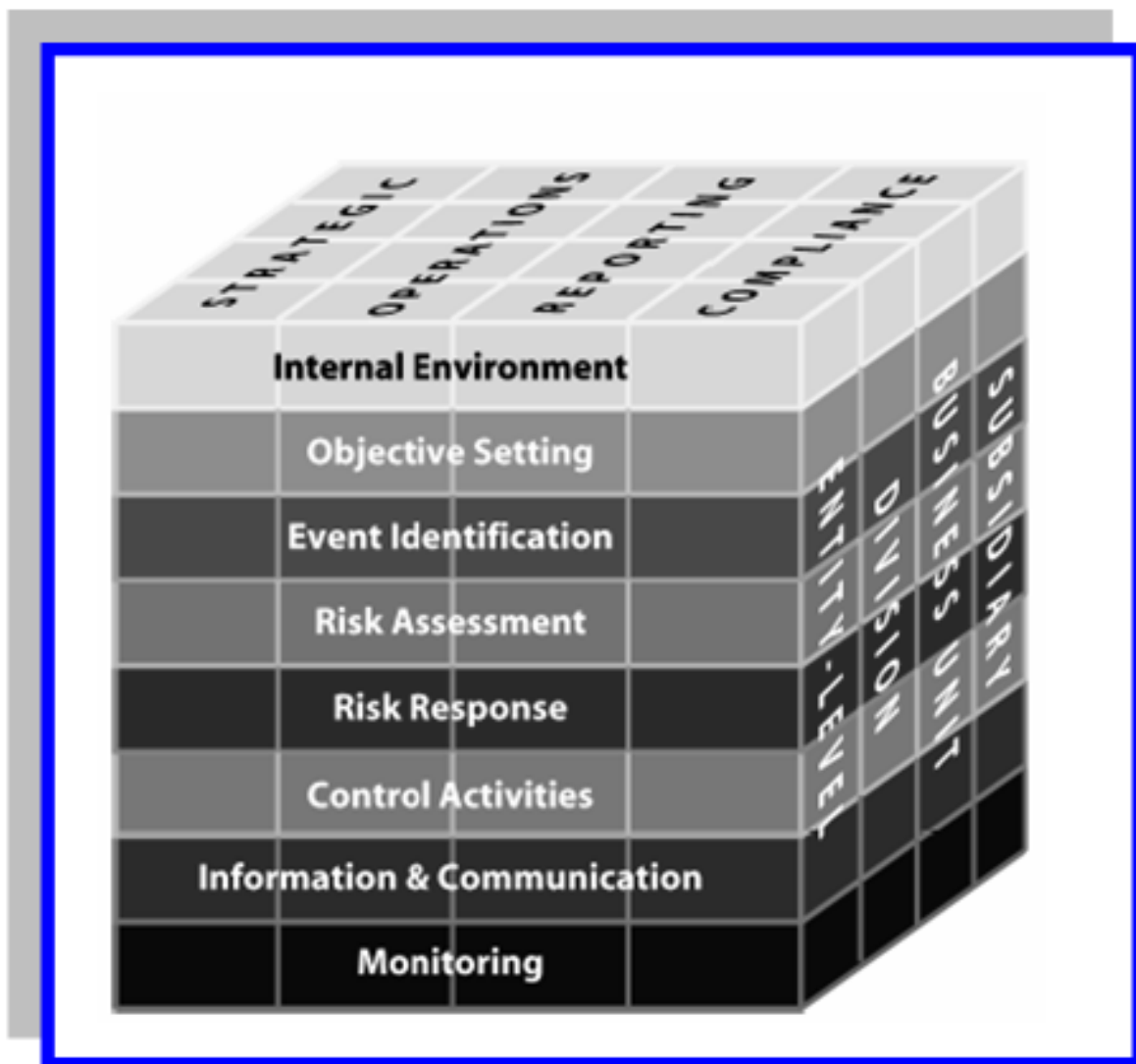
Um die Ziele zu erreichen, besteht ERM im Gegensatz zu COSO I aus acht in wechselseitiger Beziehung zueinander stehenden Komponenten (siehe Anlage 5), die in die Unternehmensprozesse zu integrieren und unternehmensspezifisch auszugestalten sind (COSO 2003: 12). Auch hier wird ausdrücklich

eine Integration in den bestehenden Unternehmensablauf empfohlen (COSO 2003: 12).

#### 6.2.2.2. Komponenten von ERM

Im Folgenden sollen nun auch hier die einzelnen Komponenten vorgestellt werden. Da COSO I als internes Kontrollsystem grundlegend in ERM enthalten ist, wird hauptsächlich auf Unterschiede in der Ausgestaltung der einzelnen Komponenten aufmerksam gemacht.

*Abbildung 21: Enterprise Risk Management Modell*



Quelle: COSO (ERM), 2003, S. 14.

Das Modell des ERM gestaltet sich wie COSO I dreidimensional.

##### 6.2.2.2.1. Internal Environment (Internes Umfeld)

Das interne Umfeld bildet auch im ERM die Basis für alle weiteren Kompo-

ponenten des Prozesses (vgl. COSO 2003: 19). Die Komponente „Kontrollumfeld“ von COSO I wurde jedoch nun zur Komponente „Internes Umfeld“ umgewandelt und bezieht sich vor allem auf die Festlegung risikopolitischer Grundsätze im Unternehmen. Dabei legt das Management eine Risikostrategie fest, die sich an der Unternehmensstrategie auszurichten hat. Die Risikostrategie wiederum beinhaltet Vorgaben für die Identifizierung, Bewertung und Steuerung von Risiken sowie die Bestimmung der Toleranzgrenze, bis zu der Risiken akzeptiert werden, um Mehrwert im Unternehmen zu generieren (vgl. COSO 2003: 20). Die Toleranzgrenze sollte sich an den Wachstums- und Renditezielen des Unternehmens orientieren. Damit die Risikostrategie auch umgesetzt wird, ist es notwendig, bei allen Mitarbeitern ein Risikobewusstsein zu schaffen und im Unternehmen eine Risikokultur zu etablieren. Von besonderer Bedeutung ist dabei, dass die Risikostrategie nicht nur vom Management von oben nach unten kommuniziert wird, sondern auch selbst vom Management „gelebt“ wird. Nur so wird ein bewusster Umgang mit Risiken auch bei allen Mitarbeitern im Unternehmen akzeptiert. Weitere Bestandteile des internen Umfeldes sind die ethischen Werte, die Personalpolitik, die Festlegung von Verantwortlichkeiten und Kompetenzen sowie der Führungsstil, die weitestgehend dem Inhalt von COSO I entsprechen (vgl. COSO 2003: 24ff).

#### 6.2.2.2.2. Objective Setting (Zielbestimmung)

Die zweite Komponente des ERM heißt Zielbestimmung und ist in dieser Form nicht in COSO I zu finden. Die Bestimmung von Zielen ist jedoch laut ERM eine notwendige Voraussetzung für die wirksame Risikoidentifikation, Risikobewertung sowie Risikosteuerung (vgl. COSO 2003: 29). Erst nachdem Ziele für das Unternehmen definiert wurden, ist es möglich, Risiken aufzuzeigen und Steuerungsmaßnahmen vorzunehmen. Die Ziele wiederum müssen messbar sein, sie sollten mit der maximalen Risikoakzeptanz des Unternehmens im Einklang stehen und sich an der Risikostrategie ausrichten. Des Weiteren ist es wichtig, dass die Ziele von Mitarbeitern auf allen Unternehmensebenen verstanden und Risikotoleranzgrenzen festgelegt werden, um die Zielerreichung zu gewährleisten.

Zudem müssen die strategischen Oberziele auf die einzelnen Hierarchieebenen des Unternehmens herunter gebrochen und Unterziele geschaffen werden. Beispielsweise kann das Hauptziel Operations in die Ziele einer Qualitätssteigerung, einer Verkürzung von Umlaufzeiten oder einer technologischen Erneuerung unterteilt werden. Beim Reporting gilt es auf Vollständigkeit, Wahrheitsgehalt sowie Pünktlichkeit zu achten. Um Compliance zu gewährleisten, müssen die Unternehmen beispielsweise auf die neuesten Steuer- und Umweltgesetze achten (vgl. COSO 2003: 33f). Als ein weiteres Ziel setzen sich viele Unternehmen auch die Sicherung ihres Vermögens. Bei der Zielfindung ist darauf zu achten, dass auch Zielüberschneidungen möglich sind und Prioritäten gesetzt werden (vgl. COSO 2003: 34).

#### 6.2.2.2.3. Event Identification (Ereignisidentifikation)

In dieser Komponente des ERM steht die Identifikation von Ereignissen im Mittelpunkt, die die Zielerreichung des Unternehmens sowie die Umsetzung der Strategie beeinflussen. Ereignisse mit einer negativen Auswirkung auf das Unternehmen stellen Risiken dar und erfordern eine Bewertung und Steuerung. Ereignisse mit einer positiven Auswirkung können Risiken ausgleichen oder Chancen für das Unternehmen bedeuten (vgl. COSO 2003: 38). Aufgabe des Managements ist es, frühzeitig alle externen und internen Faktoren zu untersuchen, die den Eintritt eines Ereignisses auslösen. Als externe Faktoren werden beispielhaft Markt- und Wettbewerbsveränderungen, Naturkatastrophen und politische sowie demographische Veränderungen genannt (vgl. COSO 2003: 39). Intern können unverhofft hohe Reparaturkosten auftreten oder Personalrisiken entstehen. Die Identifikation der möglichen zukünftigen Ereignisse soll dabei auf alle Unternehmensbereiche ausgerichtet werden. Als Hilfsmittel zur Risikoidentifikation können beispielsweise Workshops, Interviews und Frühwarnsysteme dienen (vgl. COSO 2003: 40ff). Bei allen Identifikationsmethoden soll jedoch darauf geachtet werden, dass Vergangenheitswerte und Frühwarnindikatoren gleichermaßen Beachtung finden, um eine bessere Basis für die Risikobewertung zu ermöglichen (vgl. COSO 2003: 40). Da Risiken nicht nur isoliert auftreten, sollen auch mögliche Interdependenzen zwischen den Risiken untersucht werden. Dafür ist es sinnvoll, die Ereignisse über die Unternehmensebenen hinweg und innerhalb einzelner operativer Einheiten zu aggregieren (vgl. COSO 2003: 42). Die Ereignisidentifikation bildet wiederum die Ausgangsbasis für die Risikobewertung.

#### 6.2.2.2.4. Risk Assessment (Risikobewertung)

Die Risikobewertung ermöglicht einem Unternehmen, sich ein genaues Bild von dem Ausmaß zu verschaffen, inwieweit potenzielle Ereignisse die Erreichung der Unternehmensziele positiv oder negativ beeinflussen können (vgl. COSO 2003: 47). Eine Risikobewertung soll sowohl bezüglich des inhärenten als auch des Restrisikos erfolgen, was bedeutet, dass Risiken sowohl vor der Einleitung von Steuerungsmaßnahmen als auch nach der Maßnahmendurchführung bewertet werden sollen (vgl. COSO 2003: 47). Die Bewertung findet dabei unter zwei Aspekten statt. So wird zum einen die Wahrscheinlichkeit, dass ein bestimmtes Ereignis eintritt, betrachtet und zum anderen das Ausmaß dieses Ereignisses untersucht. Zu berücksichtigen sind dabei sowohl qualitative als auch quantitative Faktoren (vgl. COSO 2003: 48). Quantitative Bewertungsverfahren verlangen ein hohes Maß an mathematischen Kenntnissen wie beispielsweise der VAR. Der Vorteil dieser Methode besteht jedoch in der möglichen Berücksichtigung von Interdependenzen zwischen den Risiken (vgl. COSO 2003: 50). Es werden aber auch Szenarioanalysen oder eine visuelle Darstellung in Form einer Risikomatrix empfohlen. Nach erfolgter Bewer-

tung können Maßnahmen zur Risikosteuerung abgeleitet werden (vgl. COSO 2003: 50).

#### 6.2.2.2.5. Risk Response (Risikosteuerung)

Nach der Bewertung gilt es Steuerungsmaßnahmen für die Risiken festzulegen, die die erwarteten Eintrittswahrscheinlichkeiten und Auswirkungen der Risiken in den unternehmenseigenen Rahmen der Risikotoleranz bringen (vgl. COSO 2003: 53). Das ERM empfiehlt die Risikovermeidung, die Risikoverminderung, die Risikoteilung (Risikotransfer) und die Risikoakzeptanz (vgl. COSO 2003: 53ff) als Gegensteuerungsmaßnahmen wie sie bereits im Rahmen dieser Arbeit beschrieben wurden und hier deshalb nicht weiter erläutert werden. Bei der Auswahl der Maßnahme ist die generelle Risikobereitschaft des Unternehmens, das Kosten-Nutzen-Verhältnis zwischen Risiko und Reaktion sowie die Eignung der Maßnahmen zur Risikobewältigung zu berücksichtigen (vgl. COSO 2003: 55).

Die Entscheidung für eine Steuerungsmaßnahme liegt letztendlich im Ermessen des Managements. Zu beachten ist, dass meistens nach den Steuerungsmaßnahmen Restrisiken vorhanden bleiben, die einer weiteren Beobachtung und Bewertung unterliegen müssen (vgl. COSO 2003: 57).

#### 6.2.2.2.6. Control Activities (Kontrollaktivitäten)

Kontrollaktivitäten sind Grundsätze und Verfahren, die das Unternehmen unterstützen, die Wirksamkeit der Risikosteuerungsmaßnahmen sicherzustellen (vgl. COSO 2003: 60), um in der Folge die Zielerreichung zu gewährleisten. Dies kann beispielsweise erfolgen, indem die Einhaltung von Verfahren und Richtlinien unternehmensweit überwacht wird. Kontrollaktivitäten finden im gesamten Unternehmen, auf allen Ebenen und für alle Funktionen statt. Sie sind damit prozessintegriert und umfassen eine große Bandbreite an Tätigkeiten wie Genehmigung, Berechtigung, Verifizierung, Abstimmung, Überprüfung der Betriebsleitung, Schutz des Vermögens und die Trennung von Verantwortlichkeiten (vgl. COSO 2003: 62).

#### 6.2.2.2.7. Information and Communication (Information und Kommunikation)

Relevante Informationen finanzieller und nicht-finanzieller Art müssen übersichtlich, zeitnah und korrekt kommuniziert werden. Informationen werden auf allen Ebenen des Unternehmens benötigt, um den Mitarbeitern die Erfüllung ihrer Aufgaben zu ermöglichen und die Einhaltung der Unternehmensstrategie zu gewährleisten. Nur die Kommunikation von Risiken ermöglicht auch die rechtzeitige Durchführung von Gegensteuerungsmaßnahmen (vgl. COSO 2003: 68). Als Kommunikationsmittel können Berichte in Papierform, E-Mails, computergestützte Informationssysteme, Videobänder oder auch Gespräche dienen (vgl. COSO 2003: 76). Inhaltlich werden sowohl interne Daten

wie Absatzzahlen, identifizierte Risiken sowie Schadensausmaß der Risiken, als auch externe Daten in die Berichterstattung aufgenommen (vgl. COSO 2003: 73). Die Kommunikation erfolgt dabei sowohl von oben nach unten (Top-down) im Unternehmen als auch von unten nach oben (Bottom-up). Mitarbeiter sind demnach ebenso aufgefordert, Schwachstellen im ERM an übergeordnete Hierarchiestufen zu melden.

Doch nicht nur der internen Kommunikation kommt eine große Bedeutung zu, sondern auch der Austausch mit Kunden, Anteilseignern und Lieferanten ist für ein Unternehmen wichtig, um frühzeitig auf Veränderungen reagieren zu können (vgl. COSO 2003: 75f).

#### 6.2.2.2.8. Monitoring (Überwachung)

Die Überwachungskomponente stellt die Effektivität des ERM sicher und überprüft, ob das Enterprise Risk Management auf allen Ebenen im Unternehmen durchgeführt wird. Eine Überwachung ist zudem notwendig, weil sich die Unternehmens- und Umweltbedingungen in einem ständigen Wandel befinden und derzeitige wirksame Risikosteuerungsmaßnahmen schon bald nicht mehr effektiv sein können. Die Aktivitäten umfassen dabei eine permanente Überwachung sowie eine einzelfallabhängige Prüfung des ERM oder eine Kombination aus beidem. So soll beispielsweise gewährleistet werden, dass das Risikoprofil eines Unternehmens seiner Risikobereitschaft entspricht. Die Überwachung findet im Rahmen der regulären Geschäftsausübung statt und umfasst regelmäßige Management- und Aufsichtstätigkeiten. Umfang und Häufigkeit der einzelfallabhängigen Prüfung hängt von der Effektivität der kontinuierlichen Überwachungsmaßnahmen ab (vgl. COSO 2003: 74ff).

Wie schon bei COSO I kann auch eine effektive und effiziente Implementierung des ERM-Konzeptes im Unternehmen keinen Erfolg in der Handhabung von Risiken garantieren. Zum einen ist die Prognostizierung zukünftiger Risiken immer mit Unsicherheit verbunden und zum anderen sind menschliche Fehlentscheidungen im Unternehmen nicht auszuschließen.

Beide Rahmenwerke (COSO I und ERM) sind damit theoretische Modelle, die mit Handlungsempfehlungen unterlegt und unternehmensspezifisch umzusetzen sind (vgl. Heese 2003: 226).

Nachdem nun das Enterprise Risk Management in seinen wesentlichen Grundzügen vorgestellt wurde, kommt es im nächsten Abschnitt der Arbeit zu einer Gegenüberstellung aller Risikomanagementkonzeptionen (betriebswirtschaftliches Risikomanagement, IDW PS 340, COSO I, ERM) anhand ausgewählter Kriterien.

#### 6.2.2.3. Vergleich mit COSO I, IDW PS 340 sowie dem betriebswirtschaftlichen Risikomanagement

Stellt man das Enterprise Risk Management den anderen in dieser Arbeit vorgestellten Konzeptionen in einer tabellarischen Übersicht gegenüber (siehe



Abbildung 22), so wird deutlich, dass das ERM die größten Gemeinsamkeiten mit dem betriebswirtschaftlichen Risikomanagement aufweist. Auch aus den Erläuterungen zum ERM im Abschnitt 6.2.2. ist bereits ersichtlich, dass das Rahmenwerk alle grundlegenden Anforderungen, die aus betriebswirtschaftlicher Sicht empfohlen werden, in sich vereint.

Das Enterprise Risk Management dient damit als guter Orientierungsrahmen für **alle** Unternehmen, um ein effektives und effizientes Risikomanagementsystem zu implementieren.

Der Abbildung 22 ist außerdem zu entnehmen, dass nur mit dem KonTraG in Deutschland eine gesetzliche Pflicht zur Einführung eines Risikofrüherkennungssystems besteht. Diese Besonderheit ergibt sich jedoch nicht nur im Vergleich zu den COSO-Rahmenwerken aus den USA, sondern weltweit ist in keinem anderen Land eine solche gesetzliche Verankerung vorhanden (vgl. Sitt 2003: 17).

Abbildung 22: Gegenüberstellung aller Risikomanagementkonzeptionen

| <b>Vergleichskriterien</b>                                     | Betriebswirtschaftliches Risikomanagement                                   | Risikofrüherkennungs- und Überwachungssystem nach KonTraG + IDW PS 340 | COSO I Internal Control – Internal Framework            | ERM Enterprise Risk Management  |
|--|---|--|---|---|
| <b>Rechtswirkung:</b>  | keine   | <b>Gesetzeskraft Prüfungsstandard</b>                                  | <b>keine, “Code of Best Practise”</b>                   | <b>keine, “Code of Best Practise”</b>   |
| <b>Anwendungsbereich:</b>                                      | alle Unternehmen  | <b>Aktiengesellschaften</b>  | <b>alle Unternehmen</b>                                 | <b>alle Unternehmen</b>   |
| <b>Integration in den Unternehmensprozess:</b>                 | Ja  | <b>Ja/Nein</b>   | <b>Ja</b>   | <b>Ja</b>   |
| <b>Identifikation:</b>   | alle Chancen und Risiken  | <b>bestandsgefährdende und wesentliche Risiken</b>                     | <b>alle Risiken</b>                                     | <b>alle Chancen und Risiken</b>   |
| <b>Berücksichtigung von Interdependenzen zwischen Risiken:</b> | Ja  | <b>Ja</b>  | <b>Nein</b>   | <b>Ja</b>   |
| <b>Risikosteuerungsmaßnahmen:</b>                              | Risikovermeidung<br>Risikoverminderung<br>Risikotransfer<br>Risikoakzeptanz | <b>keine, liegt im Ermessen des Vorstandes</b>                         | <b>keine, liegt im Ermessen der Unternehmensleitung</b> | <b>Risikovermeidung<br/>Risikoverminderung<br/>Risikotransfer<br/>Risikoakzeptanz</b> |
| <b>Externe Risikoberichterstattung</b>                         | kein Bestandteil  | ist Bestandteil  | nur finanzielle Berichterstattung                       | ist Bestandteil   |

Quelle: Eigene Darstellung.

## 7. Zusammenfassung und Ausblick

National wie international steht man dem Problem eines effizienten und effektiven Umgangs mit Risiken gegenüber. Da unternehmerisches Handeln immer mit Risiken verbunden ist, müssen diese so gesteuert werden, dass das Unternehmen dauerhaft seine Existenz erhalten und seine Ziele erreichen kann. Dazu leistet ein funktionsfähiges Risikomanagement einen erheblichen Beitrag. Risikobehaftete Entwicklungen werden frühzeitig erkannt und analysiert, so dass Gegensteuerungsmaßnahmen rechtzeitig eingeleitet werden können, um das Unternehmen vor einer Krise zu bewahren.

Über diese außerordentliche Bedeutung eines Risikomanagementsystems für ein Unternehmen sind sich die betriebswirtschaftliche Theorie, die Gesetzgebung und die Wirtschaftsprüferpraxis einig. Allerdings bestehen unterschiedliche Ansichten über die Anforderungen an ein solches System. Selbst in der betriebswirtschaftlichen Literatur sind unterschiedliche Konzeptionen vorhanden und man hat noch zu keiner allgemeingültigen Lösung gefunden. Dies wird meist damit begründet, dass ein Risikomanagement von der Größe, Struktur und Branche eines Unternehmens abhängig und damit unternehmensindividuell auszugestalten ist.

Da in Deutschland mit dem KonTraG seit 1998 für bestimmte Unternehmen auch eine gesetzliche Pflicht zur Einrichtung und Prüfung eines Risikofrüherkennungssystems besteht, haben Wirtschaftsprüfer versucht, grundlegende Anforderungen an ein Risikofrüherkennungssystem zusammenzufassen und damit einen Prüfungsstandard zu schaffen. Daraus entwickelte sich schließlich der IDW PS 340. Wie im Abschnitt 6.2.1.1. bereits herausgestellt wurde, spiegeln sich in diesem Prüfungsstandard unter anderem auch Eigeninteressen der Abschlussprüfer wider. So sind sie vor allem an einer leichten Prüfungsfähigkeit des Risikomanagements interessiert und es besteht damit die Gefahr, dass eine betriebswirtschaftlich sinnvolle Ausgestaltung für die Unternehmen in den Hintergrund rückt.

Auch international wird versucht, das Risikomanagement mit seinen wesentlichen Inhalten abzubilden. Hier hat insbesondere COSO mit dem Enterprise Risk Management einen Standard geschaffen, der sämtliche betriebswirtschaftlichen Erkenntnisse in sich vereint und damit für alle Unternehmen zur Implementierung eines Risikomanagements ein geeignetes Rahmenwerk zur Verfügung stellt.

Da bereits COSO I international weit reichende Akzeptanz gefunden hat und in viele Prüfungsstandards aufgenommen wurde, ist davon auszugehen, dass auch COSO II zukünftig hinreichende Anerkennung finden wird. So werden Unternehmen demnächst ein Risikomanagement nachweisen müssen, das den Ansprüchen des ERM genügt.

## Anlage 1: Beispiel eines Risikoinventars

| Risikobereiche                                    |   | Risikobeschreibung                                 | Risiko-<br>ursprung | Bewertung des<br>maximalen<br>Verlustpotenzial | Priorität |
|---|---|--|---------------------|--|-----------|
| <b>Allgemeine<br/>externe Risiken</b>             | Gesetzliche Vorschriften<br>Technologie<br>Naturgewalten<br>Politische Verhältnisse | Erhöhung der MwSt.<br>führt zu Absatzrück-<br>gang | extern              | existenz-<br>gefährdend                        | hoch      |
| <b>Leistungs-<br/>wirtschaftliche<br/>Risiken</b> | Beschaffung<br>Produktion<br>Absatz<br>Forschung/Entwicklung<br>Brandschutz<br>EDV  |  |                     |  |           |
| <b>Finanzwirt-<br/>schaftliche<br/>Risiken</b>    | Kundenbonität<br>Liquidität<br>Marktpreisentwicklung                                |  |                     |  |           |
| <b>Risiken aus<br/>Unternehmens-<br/>führung</b>  | Organisation<br>Führungsstil<br>Unternehmenskultur<br>Personalrisiken               |  |                     |  |           |

Quelle: In Anlehnung an Romeike (2003: 179).

## Anlage 2: Vergleich von VAR und Risikomatrix

| Unterscheidungsmerkmale  | Value at Risk   | Risikomatrix  |
|--|---|---|
| Risikobezugsmaß  | <ul style="list-style-type: none"> <li>• Der Value at Risk kennzeichnet den maximalen Verlust, der innerhalb eines vorgegebenen Zeitraums eintreten kann.</li> <li>• Der Fokus liegt auf dem Gesamtrisiko (über alle Risiken/Risikokategorien/Unternehmensstufen aggregierbar).</li> </ul>  | <ul style="list-style-type: none"> <li>• Die Risikomatrix hebt auf wichtige Einzelrisiken der jeweiligen Unternehmensebene ab.</li> <li>• Eine Gesamtrisikoposition (über alle Unternehmensstufen hinweg) lässt sich nicht darstellen.</li> </ul>   |
| Risikoanalyse (umfasst Identifikation und Bewertung der Risiken) | <ul style="list-style-type: none"> <li>• Unterscheidung zweier Risikoarten: Ereignisorientierte Risiken (z.B. Eintrittswahrscheinlichkeit 30%, Schadenshöhe: 500.000€)</li> <li>• Verteilungsorientierte Risiken (d.h. Verteilungsfunktion für Risiko erforderlich) – umfangreiche Identifikation notwendig</li> <li>• im Idealfall: Identifikation und Bewertung sämtlicher Korrelationen (d.h. Aufstellung einer Korrelationsmatrix)</li> </ul> | <ul style="list-style-type: none"> <li>• nur ereignisorientierte Risiken (i.d.R. ohne Korrelationen)</li> </ul>   |
| Risikoaggregation  | <ul style="list-style-type: none"> <li>• standardisiertes Vorgehen der Risikoaggregation</li> <li>• teilweise aufwendige mathematische/statistische Rechenalgorithmen</li> <li>• Gesamtrisikoposition über alle Risiken/Risikokategorien (über alle Unternehmensstufen) hinweg er-rechenbar</li> </ul>  | <ul style="list-style-type: none"> <li>• keine zwingend vorgegebene Vorgehensweise</li> <li>• Gefahr des subjektiven Vorgehens</li> <li>• Risikoaggregation nur innerhalb von Risikokategorien möglich (z.B. Zusammenfassung aller gleichartigen „Wechselkursrisiken“)- keine Gesamtrisikoposition</li> </ul> |
| Risikoberichterstattung/-kommunikation                           | <ul style="list-style-type: none"> <li>• Kommunikation von Risiken bei Überschreitung so genannter „Limits“ (mit Wesentlichkeitsgrenzen vergleichbar)</li> <li>• Risikoverteilungskurve (auf Basis des Value at Risk) als Kommunikationsinstrument</li> </ul>   | <ul style="list-style-type: none"> <li>• Kommunikation von Risiken bei Überschreitung der Wesentlichkeitsgrenzen einzelner Betrachtungsbereiche</li> <li>• Risikomatrix als Kommunikationsinstrument</li> </ul>   |
| Akzeptanz bei Umsetzung  | <p>(Anfangs ) gering, da:</p> <ul style="list-style-type: none"> <li>• statistische Modelle anspruchsvoll</li> <li>• schwierig handhabbar/hoher Erstellungsaufwand</li> <li>• Black-Box-Algorithmus nicht nachvollziehbar</li> </ul>  | <p>Hoch, da</p> <ul style="list-style-type: none"> <li>• Risikomatrix grafisch leicht nachvollziehbar</li> <li>• einfach handhabbar/geringer Erstellungsaufwand</li> <li>• kein Verrechnungsalgorithmus (hohe Transparenz)</li> </ul>   |

Quelle: Wolf, K., 2002, S. 1732.

### Anlage 3: Gegenüberstellung aller gesetzlichen Neuerungen

| Paragraph                            | vor KonTraG  | KonTraG   | TransPuG  | BilReG   |
|--------------------------------------|--|---|---|--|
| § 91 Abs. 2 AktG                     | nicht vorhanden  | „Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.“  |   |  |
| § 161 AktG                           | nicht vorhanden  | nicht vorhanden   | „Vorstand und Aufsichtsrat der börsennotierten Gesellschaft erklären jährlich, dass den vom BMJ im amtlichen Teil des elektronischen Bundesanzeigers bekannt gemachten <b>Empfehlungen der „Regierungskommission DCCG“</b> entsprochen wurde und wird oder welche Empfehlungen nicht angewendet wurden oder werden. Die Erklärung ist den Aktionären dauerhaft zugänglich zu machen.“ |  |
| § 289 Abs. 1 HGB<br>§ 315 Abs. 1 HGB | „Im (Konzern-) Lagebericht sind zumindest der Geschäftsverlauf und die Lage (des Konzerns) der Kapitalgesellschaft so darzustellen, dass ein den tatsächlichen Verhältnissen entsprechendes Bild vermittelt wird.“ | „Im (Konzern-) Lagebericht sind zumindest der Geschäftsverlauf und die Lage (des Konzerns) der Kapitalgesellschaft so darzustellen, dass ein den tatsächlichen Verhältnissen entsprechendes Bild vermittelt wird; <b>dabei ist auch auf die Risiken der künftigen Entwicklung einzugehen.</b> “ | <b>beibehalten</b>  | „Im Lagebericht sind der Geschäftsverlauf einschließlich der Geschäftsergebnisse und die Lage der Kapitalgesellschaft so darzustellen, dass ein den tatsächlichen Verhältnissen entsprechendes Bild vermittelt wird. Er hat eine ausgewogene und umfassende, dem Umfang und der Komplexität der Geschäftstätigkeit entsprechende Analyse des Geschäftsverlaufs und der Lage der Gesellschaft zu enthalten. In die Analyse sind die für die Geschäftstätigkeit bedeutsamsten finanziellen Leistungsindikatoren einzubeziehen und unter Bezugnahme auf die im Jahresabschluss ausgewiesenen Beträge und Angaben zu erläutern. Ferner sind im Lagebericht die wesentlichen Ziele und Strategien der gesetzlichen Vertreter für die Kapitalgesellschaft zu beschreiben <b>sowie die voraussichtliche Entwicklung mit ihren wesentlichen Chancen und Risiken zu beurteilen und zu erläutern, zugrunde liegende Annahmen sind anzugeben.</b> “ |

|                                     |  |   |  |  |
|-------------------------------------|--|---|--|--|
| <p>§ 317<br/>Abs.<br/>2<br/>HGB</p> | <p>Der Lagebericht wurde auf eine „nicht falsche Darstellung“ geprüft.</p> | <p>„Der Lagebericht und der Konzernlagebericht sind darauf zu prüfen, ob der Lagebericht mit dem Jahresabschluss und der Konzernlagebericht mit dem Konzernabschluss sowie mit den bei der Prüfung gewonnenen Erkenntnissen des Abschlussprüfers in Einklang stehen und ob der Lagebericht insgesamt eine zutreffende Vorstellung von der Lage des Unternehmens und der Konzernlagebericht insgesamt eine zutreffende Vorstellung von der Lage des Konzerns vermittelt. <b>Dabei ist auch zu prüfen, ob die Risiken der künftigen Entwicklung zutreffend dargestellt sind.</b>“</p> |  | <p>„Der Lagebericht und der Konzernlagebericht sind darauf zu prüfen, ob der Lagebericht mit dem Jahresabschluss, ggf. auch mit dem Einzelabschluss nach § 325 Abs. 2a, und der Konzernlagebericht mit dem Konzernabschluss sowie mit den bei der Prüfung gewonnenen Erkenntnissen des Abschlussprüfers in Einklang stehen und ob der Lagebericht insgesamt eine zutreffende Vorstellung von der Lage des Unternehmens und der Konzernlagebericht insgesamt eine zutreffende Vorstellung von der Lage des Konzerns vermittelt. <b>Dabei ist auch zu prüfen, ob die Chancen und Risiken der künftigen Entwicklung zutreffend dargestellt sind.</b>“</p> |
| <p>§ 317<br/>Abs.<br/>4<br/>HGB</p> | <p><b>nicht vorhanden</b></p>  | <p>„Bei einer Aktiengesellschaft, die Aktien mit amtlicher Notierung ausgegeben hat, ist außerdem im Rahmen der Prüfung zu beurteilen, ob der Vorstand die ihm nach § 91 Abs.2 des Aktiengesetzes obliegenden Maßnahmen in einer geeigneten Form getroffen hat und das danach einzurichtende Überwachungssystem seine Aufgaben erfüllen kann.“</p>  | <p>„Bei einer börsennotierten Aktiengesellschaft ist außerdem im Rahmen der Prüfung zu beurteilen, ob der Vorstand die ihm nach § 91 Abs.2 des Aktiengesetzes obliegenden Maßnahmen in einer geeigneten Form getroffen hat und das danach einzurichtende Überwachungssystem seine Aufgaben erfüllen kann.“</p> |  |

## **Anlage 4: Risikomanagementhandbuch**

### **Beispielhafte Gliederung eines Risikomanagementhandbuchs**

#### 1. Vorwort

- 1.1. Was ist Risikomanagement?
- 1.2. Bedeutung der frühzeitigen Erkennung von Risiken für XY AG
- 1.3. Zielsetzung der Dokumentation

#### 2. Das Risikomanagementsystem der XY AG

##### 2.1. Definitionen

- 2.1.1. Risiko
- 2.1.2. Risikofelder; Kategorisierung von Risiken
- 2.1.3. Bestands gefährdende und wesentliche Risiken

##### 2.2. Risikopolitische Grundsätze

##### 2.3. Aufbau und Organisation

- 2.3.1. Verantwortliche und ihre Funktionen
  - 2.3.1.1. Vorstand
  - 2.3.1.2. Interne Revision
  - 2.3.1.3. Controlling
  - 2.3.1.4. Risikomanagement-Arbeitsgruppe
  - 2.3.1.5. Sonstige Verantwortliche

##### 2.4. Ablauf des Risikomanagementprozesses

- 2.4.1. Risikoidentifikation
  - 2.4.1.1. Methoden der Risikoidentifikation
  - 2.4.1.2. Plausibilitätsprüfung
- 2.4.2. Risikobewertung
  - 2.4.2.1. Verfahren der Risikoquantifizierung
  - 2.4.2.2. Bewertung und Meldung von Einzelrisiken
  - 2.4.2.3. Aggregation der Einzelrisiken zur Konzernrisikoermittlung
  - 2.4.2.4. Risikoportfolio als Ergebnis
- 2.4.3. Risikosteuerung
  - 2.4.3.1. Risikovermeidung
  - 2.4.3.2. Risikoverminderung
  - 2.4.3.3. Risikotransfer
  - 2.4.3.4. weitere Maßnahmen
- 2.4.4. Risikokommunikation
  - 2.4.4.1. Unterjährige Berichterstattung
  - 2.4.4.2. Integration in bestehendes Berichtswesen
- 2.4.5. Risikoüberwachung
  - 2.4.5.1. Umfang der Risikoüberwachung
  - 2.4.5.2. Interne Revision und Controlling

#### 3. Anpassungsfähigkeit des Risikomanagements an sich wandelnde Umfeldbedingungen

Quelle: In Anlehnung an Seidel (2002: 323f).



## Anlage 5: Komponenten des Enterprise Risk Managements



Quelle: COSO (Enterprise Risk Management) Executive Summary (2004: 15).

## Literaturverzeichnis

- Alquen, K.** (1999): Risikomanagement: Unternehmensrisiken erkennen und bewältigen, Eschborn 1999.
- Bartram, S. M.** (2000): Finanzwirtschaftliches Risiko, Exposure und Risikomanagement von Industrie- und Handelsunternehmen, in: WiSt, 2000, Heft 5, S. 242 – 249.
- Basler Ausschuss für Bankenaufsicht** (1998): Rahmenkonzept für Interne Kontrollsysteme in Bankinstituten, Basel 1998.
- Baumeister, A./Freisleben, N.** (2003): Prüfung des Risikomanagements und Risikolageberichts – Ziele und Umsetzung von Prüfkonzepten, in: Entwicklungen der Wirtschaftsprüfung, Hrsg. Richter, M., Bielefeld 2003, S. 17 – 93.
- Beinert, C.** (2003): Bestandsaufnahme Risikomanagement, in: Risikomanagement und Rating, Hrsg.: Reichling, P., Wiesbaden 2003, S. 21 – 41.
- Bitz, H.** (2000a): Abgrenzung des Risiko-Frühwarnsystems i.e.S. nach KonTraG zu einem umfassenden Risiko-Managementsystem im betriebswirtschaftlichen Sinn, in: BFuP, 52. Jg. 2000, Heft 3, S. 231 – 241.
- Bitz, H.** (200b): Risikomanagement nach KonTraG: Einrichtung von Frühwarnsystemen zur Effizienzsteigerung und zur Vermeidung persönlicher Haftung, Stuttgart 2000.
- Böcking, H.-J./Orth, C.** (1998): Kann das “Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)” einen Beitrag zur Verringerung der Erwartungslücke leisten? : Eine Würdigung auf Basis von Rechnungslegung und Kapitalmarkt, in: Die Wirtschaftsprüfung, 51. Jg. 1998, Heft 8, S. 351 – 364.
- Böcking, H.-J./Orth, C.** (2000): Risikomanagement und das Testat des Abschlussprüfers, in: BFuP, 52. Jg. 2000, Heft 3, S. 242 – 260.
- Brebeck, F./Herrmann, D.** (1997): Zur Forderung des KonTraG-Entwurfs nach einem Frühwarnsystem und zu den Konsequenzen für die Jahres- und Konzernabschlussprüfung, in: Die Wirtschaftsprüfung, 50. Jg. 1997, Heft 12, S. 381 – 391.
- Brühwiler, B.** (2001): Unternehmensweites Risk Management als Frühwarnsystem: Methoden und Prozesse für die Bewältigung von Geschäftsrisiken in integrierten Managementsystemen, Bern, Stuttgart 2001.
- BT-Drucksache** 13/9712 vom 28.01.1998.
- Burger, A./Buchhart, A.** (2002): Risiko-Controlling, München/Wien 2002.
- Buderath, H. M.** (2003): Das Interne Kontrollsystem in einem internationalen Unternehmen, in: WPg- Sonderheft, 2003, S. 219 – 223.
- Buderath, H. M.** (2004): Auswirkungen des Sarbanes-Oxley-Acts auf die Interne Revision, in: BFuP, 2004, Heft 1, S. 39 – 50.
- COSO** (1992): Internal Control – Integrated Framework, Two-volume edition, New York 1992.
- COSO** (2003): Enterprise Risk Management, Draft, 2003.
- COSO** (2004): Enterprise Risk Management, Executive Summary, 2004.
- Dahms, S.** (2003): Risikoinventar, in: Risikomanagement und Rating, Hrsg.: Reichling, P., Wiesbaden 2003, S. 215 – 230.
- Diederichs, M./Reichmann, T.** (2003): Risikomanagement und Risiko- Controlling in der

- Praxis – Ergebnisse einer empirischen Untersuchung, 2003, Heft 5, S. 229 – 234.
- Diederichs, M./Form, S./Reichmann, T.** (2004): Standard zum Risikomanagement, in: Controlling-Spezial, 2004, Heft 4/5, S. 189-198.
- Dörner, D./Bischof, S.** (1999): Zweifelsfragen zur Berichterstattung über die Risiken der künftigen Entwicklung im Lagebericht, in: Die Wirtschaftsprüfung, 52. Jg. 1999, Heft 12, S. 445 – 455.
- Eichler, H./Bungartz, O.** (2004): Enterprise Risk Management – aktuelle Entwicklungen im Bereich unternehmensinterner Risiko- und Überwachungssysteme, in: Interne Revision, 39. Jg. 2004, Heft 3, S. 108 – 113.
- Emmerich, G.** (1999): Risikomanagement in Industrieunternehmen – gesetzliche Anforderungen und Umsetzung nach dem KonTraG, in: ZfbF, 51. Jg. 1999, H. 11, S. 1075 – 1089.
- Ettmüller, K.** (2003): Risikomanagement in der BASF-Gruppe: Rechtliche Grundlagen, praktische Ausgestaltung und Prüfung, in: Controlling, 2003, Heft 12, S. 689 - .....
- Ferlings, J./Lanfermann, G.** (2002): Unabhängigkeit von deutschen Abschlussprüfern nach Verabschiedung des Sarbanes-Oxley Act, in: Der Betrieb, 55. Jg. 2002, Heft 41, S. 2117 – 2122.
- Gampenrieder, P./Greiner, M.** (2002): Risikomanagement als gesetzliche Forderung an mittelständische Unternehmen, in: krp, 46. Jg. 2002, Heft 5, S. 283 – 289.
- Gleißner, W.** (2000): Risikopolitik und Strategische Unternehmensführung, in: Der Betrieb, 53. Jg. 2000, Heft 33, S. 1625 – 1629.
- Hakelmacher, S.** (2001): Die korpulente Gouvernante II – Corporate Governance mit Aussicht auf KonTraG II, in: Die Wirtschaftsprüfung, 54. Jg. 2001, Heft 4, S. 177 – 187.
- Hartmann, S.** (2003): Risikomanagement als Führungsaufgabe von Unternehmen, Wissenschaftliche Arbeitsberichte des ZWW, Hrsg.: Kahle, E./Merkel, W./Simon, J., Lüneburg 2003.
- Heese, K.** (2003): Der risiko-, prozess- und systemorientierte Prüfungsansatz, in : WPg-Sonderheft 2003, S. 223 – 230.
- Helm, S./Risse, R.** (1999): Chancen- und Risikomanagement im Konzern Deutsche Post AG, in: krp, 43. Jg. 1999, Heft 5, S. 277 – 283.
- Hohnhorst, G.** (2002): Anforderungen an das Risikomanagement nach dem KonTraG, in: Herausforderung Risikomanagement, Hrsg.: Hölscher, R./Elfgen, R., Wiesbaden 2002, S. 91 – 108.
- Hölscher, R.** (2000): Gestaltungsformen und Instrumente des industriellen RM, in: Risk Controlling in der Praxis, Hrsg.: Schierenbeck, H., Stuttgart 2000, S. 297 – 363.
- Hölscher, R.** (2002): Von der Versicherung zur integrativen Risikobewältigung: Die Konzeption eines modernen Risikomanagements, in: Herausforderung Risikomanagement, Hrsg.: Hölscher, R./Elfgen, R., Wiesbaden 2002, S. 3 – 31.
- Hornung, K./Reichmann, T./Diederichs, M.** (1999): Risikomanagement – Teil I: Konzeptionelle Ansätze zur pragmatischen Realisierung gesetzlicher Anforderungen, in: Controlling, 11. Jg. 1999, S. 317 – 325.
- Horvath, P.** (2003a): Controlling, 9., vollständig überarbeitete Auflage, München 2003a.

- Horvath, P.** (2003b): Anforderungen an ein modernes Internes Kontrollsystem, in: WPg-Sonderheft 2003b, S. 211-218.
- IDW** (1998) Rechnungslegungsstandard RS HFA 1: Aufstellung des Lageberichts, in: Die Wirtschaftsprüfung, 1998, Heft 15, S. 653 – 662.
- IDW** (1999): Prüfungsstandard 340: Die Prüfung des Risikofrüherkennungssystems nach § 317 Abs. 4 HGB, in: Die Wirtschaftsprüfung, 1999, Heft 16, S. 658 – 662.
- IDW** (2001) Prüfungsstandard 260: Das interne Kontrollsystem im Rahmen der Abschlussprüfung, in: Die Wirtschaftsprüfung, 2001, Heft 16, S. 821 – 831.
- Jacob, H. J.** (2001): Die Transformation der International Standards on Auditing in deutsche Grundsätze ordnungsgemäßer Abschlussprüfung, in: Die Wirtschaftsprüfung, 54. Jg. 2001, Heft 5, S. 237 – 244.
- Kajüter, P.** (2001a): Risikoberichterstattung: Empirische Befunde und der Entwurf des DRS 5, in: Der Betrieb, 54. Jg. 2001, Heft 3, S. 105 – 111.
- Kajüter, P.** (2001b): Der Entwurf des DRS 5 zur Risikoberichterstattung, in: Die Wirtschaftsprüfung, 2001, Heft 4, S. 205 – 209.
- Kajüter, P.** (2003): Risikomanagement in internationalen Konzernen, in: Strategische und internationale Perspektiven des Managements, Hrsg. Achenbach, S./Borghoff, T./Schulte, A., Köln 2003, S. 42- 74.
- Kajüter, P.** (2004): Der Lagebericht als Instrument einer kapitalmarktorientierten Rechnungslegung, in: Der Betrieb, 57. Jg. 2004, S. 197 – 203.
- Kajüter, P./Winkler, C.** (2004): Praxis der Risikoberichterstattung deutscher Konzerne, in: Die Wirtschaftsprüfung, 57. Jg. 2004, Heft 6, S. 249 – 261.
- Kauffmann, H./Götzenberger, G.** (2003): Aufbau eines effektiven Internal Control Systems nach Section 404 des Sarbanes-Oxley Acts, in: Performancesteigerung und Kostenoptimierung: Neue Wege und erfolgreiche Praxislösungen, Hrsg.: Horvath, P., Stuttgart 2003, S. 149 – 166.
- Kindler, P./Pahlke, A.-K.** (2001): Überwachungspflichten des Aufsichtsrates, in: Risikomanagement nach dem KonTraG, Hrsg.: Lange, K.W./Wall, F., München 2001, S. 60 – 94.
- Kirchner, M.** (2002): Risikomanagement – Problemaufriss und praktische Erfahrungen unter Einbeziehung eines sich ändernden unternehmerischen Umfeldes, in: Kooperation & Wettbewerb, Band 2, Hrsg.: Kramer, J.W./Sepp, J./Boevesky, I., München und Mering 2002.
- Kirchner, M.** (2003): Checklisten zur systematischen Ermittlung und Bewertung von Chancen und Risiken, in: BC, 2003, Heft 1, S. 11-17.
- Kramer, J. W.** (2002): Vom Rechnungswesen zum Risikomanagement: Aktuelle Fragestellungen im Controlling, in: Kooperation & Wettbewerb, Band 1, Hrsg.: Kramer, J.W./Sepp, J./Boevesky, I., München und Mering 2002.
- Krystek, U.** (1999): Neue Controlling- Aufgaben durch neue Gesetze?: KonTraG und InsO als Herausforderung für das Controlling, 43. Jg. 1999, Heft 3, S. 145 – 151.
- Lanfermann, G./Maul, S.** (2002): Auswirkungen des Sarbanes-Oxley Act in Deutschland, in: Der Betrieb, 55. Jg. 2002, Heft 34, S. 1725 – 1732.

- Lanfermann, G./Maul, S.** (2003): SEC-Ausführungsregelungen zum Sarbanes-Oxley Act, in: *Der Betrieb*, 56. Jg. 2003, Heft 7, S. 349 – 355.
- Lange, K. W.** (2001): Anforderungen an die Berichterstattung über Lagebericht und Konzernlagebericht, in: *Risikomanagement nach dem KonTraG*, Hrsg.: Lange, K.W./Wall, F., München 2001, S. 131 – 159.
- Lehner, U./Schmidt, M.** (2000): Risikomanagement im Industrieunternehmen, in: *BFuP*, 52. Jg. 2000, Heft 3, S. 261 – 272.
- Liekweg, A.** (2003): *Risikomanagement und Rationalität*, Dissertation (Wissenschaftliche Hochschule für Unternehmensführung (WHU) Vallendar), Wiesbaden 2003.
- Lück, W.** (1998): Elemente eines Risiko-Managementsystems – Die Notwendigkeit eines Risiko-Managementsystems durch den Entwurf eines Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), in: *DB*, 1998, Heft 1/2, S. 8 – 14.
- Lück, W.** (2000): Managementrisiken im Risikomanagementsystem, in: *Der Betrieb*, 53. Jg. 2000, Heft 30, S. 1473 – 1477.
- Maier, H.-D.** (2001): *Risiko-Management: 14 Thesen zur risikobewussten Unternehmensführung*, Zürich 2001.
- Martin, T.A./Bär, T.** (2002): *Grundzüge des Risikomanagements nach KonTraG: das Risikomanagementsystem zur Krisenfrüherkennung nach § 91 Abs. 2 AktG*, München/Wien 2002.
- Menzies, C.** (2004): *Sarbanes-Oxley Act – Professionelles Management interner Kontrollen*, Stuttgart 2004.
- Mertin, D./Schmidt, S.** (2001): Internationale Harmonisierung der Anforderungen an die Abschlussprüfung auf der Grundlage der Verlautbarungen der IFAC, in: *Die Wirtschaftsprüfung*, 2001, Heft 6, S. 317 – 335.
- Neubeck, G.** (2003): *Prüfung von Risikomanagementsystemen*, Düsseldorf 2003.
- Niehus, R. J.** (2001): Die Zukunft der Standards des DRSC, in: *Der Betrieb*, 54. Jg. 2001, Heft 2, S. 53 – 59.
- Picot, G.** (2001): Überblick über die Kontrollmechanismen im Unternehmen nach KonTraG, in: *Risikomanagement nach dem KonTraG*, Hrsg.: Lange, K.W./Wall, F., München 2001, S. 5 – 37.
- Reichling, P.**: Aufbau und Elemente eines betrieblichen Risikomanagements, in: *Risikomanagement und Rating*, Hrsg.: Reichling, P., Wiesbaden 2003, S. 109 – 124.
- Reichmann, T./Form, S.** (2003): Instrumente des Risikomanagement und Risiko-Controlling, in: *18. Deutscher Controlling Congress*, Hrsg.: Reichmann, T., Dortmund 2003, S. 167 – 188.
- Romeike, F.** (2003a): Enterprise-wide Risk Management: Opportunities to maximise value and minimise risk, in: *Credit Management in a European Context*, Hrsg.: Verein für Credit Management e.V./Schneider-Maessen, J./Weiß, B., Heidelberg 2003, S. 171 – 184.
- Romeike, F.** (2003b): *Gesetzliche Grundlagen, Einordnungen und Trends*, Wiesbaden 2003.
- Scheffner, J./Strutz, A.** (2002): *Thesen zu einem verbesserten externen Reporting in inter-*

- nationalen Konzernen, in: krp, 46. Jg. 2002, Heft 4, S. 202 – 205.
- Schindler, J./Rabenhorst, D.** (2001): Prüfung des Risikofrüherkennungssystems im Rahmen der Abschlussprüfung, in: Risikomanagement nach dem KonTraG, Hrsg.: Lange, K.W./Wall, F., München 2001, S. 160 – 175.
- Schmalenbach-Gesellschaft** (2000) -Arbeitskreis für „Externe und interne Überwachung der Unternehmung“: Auswirkungen des KonTraG auf die Unternehmensüberwachung, in: Der Betrieb, 2000, Beilage Nr. 11 zu Heft 37, S. 1 – 11.
- Schöne, F.** (2003): Erfordernis von Risikomanagement und Rating, in: Risikomanagement und Rating, Hrsg.: Reichling, P., Wiesbaden 2003, S. 89 – 109.
- Schwarz, C./Holland, B.** (2002): Enron, Worldcom... und die Corporate-Governance-Diskussion, in: ZIP Zeitschrift für Wirtschaftsrecht, 23. Jg. 2002, Heft 37, S. 1661 – 1672.
- Seidel, U.-M.** (2002): Risikomanagement: Erkennen, Bewerten und Steuern von Risiken, München 2002.
- Sitt, A.** (2003): Dynamisches Risiko-Management: Zum unternehmerischen Umgang mit Risiken, Dissertation (Wirtschaftswissenschaftliche Fakultät der Universität Leipzig), Wiesbaden 2003.
- Strenger, C.** (2002): Corporate Governance: Entwicklung in Deutschland und internationale Konvergenz, in: Vom Financial Accounting zum Business Reporting: Kapitalmarktorientierte Rechnungslegung und integrierte Unternehmenssteuerung, Hrsg.: Küting, K./Weber, C.-P., Stuttgart 2002, S. 445 – 461.
- Strieder, T.** (2004): Erläuterungen zum Deutschen Corporate Governance Kodex, in: Finanz-Betrieb, 2004, Heft 1, S. 13 – 27.
- Vogler, M./Grundert, M.** (1998): Einführung von Risikomanagementsystemen – Hinweise zur praktischen Ausgestaltung, in: Der Betrieb, 51. Jg. 1998, Heft 34, S. 2377 – 2382.
- Vogler, M./Engelhard, S./Grundert, M.** (2000): Risikomanagementsysteme – Stand der Umsetzung, in: Der Betrieb, 53. Jg. 2000, Heft 29, S. 1425 – 1431.
- Wall, F.** (2002): Unterschiede und Gemeinsamkeiten von Risikomanagement im Rahmen der Unternehmensplanung versus Risikomanagement nach KonTraG – eine Gedankensammlung, Witten, 2002.
- Wall, F.** (2003): Kompatibilität des betriebswirtschaftlichen Risikomanagement mit den gesetzlichen Anforderungen?: Eine Analyse mit Blick auf die Abschlussprüfung, in: Die Wirtschaftsprüfung, 56. Jg. 2003, Heft 9, S. 457 – 471.
- Weber, J./Weißberger, B.E./Liekweg, A.** (1999): Risk Tracking and Reporting: unternehmerisches Chancen- und Risikomanagement nach dem KonTraG, Koblenz 1999.
- Wiedmann, H.** (1999): Ansätze zur Fortentwicklung der Abschlussprüfung, in: Die Wirtschaftsprüfung, 1999, Heft 7, S. 338 – 351.
- Wolf, K.** (2002): Potenziale derzeitiger Risikomanagementsysteme, in: DStR, 2002, Heft 40, S. 1729 – 1733.
- Wolf, K./Runzheimer, B.** (2003): Risikomanagement und KonTraG: Konzeption und Implementierung, 4. Auflage, Wiesbaden 2003.
- Wolf, K.** (2003): Stand des Risikomanagements in deutschen Unternehmen – Handlungs-

empfehlungen, in: BC, 2003, Heft 1, S. 7 – 11.

**Wolf, K.** (2004): Risikomanagement gemäß den Anforderungen des KonTraG bei Daimler Chrysler, in: Controlling-Spezial, 2004, Heft 4/5, S. 211 – 216.

**Zellmer, G.** (1990): Risiko-Management, Berlin 1990.

**Zimmer, D./Sonneborn, A.** (2001): § 91 Abs. 2 AktG - Anforderungen und gesetzgeberische Absichten, in: Risikomanagement nach dem KonTraG, Hrsg.: **Lange, K.W./Wall, F.**, München 2001, S. 38 – 59.

### **Internetseiten**

[www.bmj.de/media/archive/649.pdf](http://www.bmj.de/media/archive/649.pdf), 04.10.2004.

[www.coso.org](http://www.coso.org), 29.09.2004.

[www.risknews.de](http://www.risknews.de), 24.06.2004.

### **Autorenangaben**

Dipl.-Kauffrau (FH) Katrin Pampel

Fachbereich Wirtschaft

Hochschule Wismar

Philipp-Müller-Straße

Postfach 12 10

D – 23966 Wismar

E-mail: [KatrinPampel@web.de](mailto:KatrinPampel@web.de)

## WDP - Wismarer Diskussionspapiere / Wismar Discussion Papers

- Heft 04/2003 Jost W. Kramer: Entwicklung und Perspektiven der produktivgenossenschaftlichen Unternehmensform
- Heft 05/2003 Jost W. Kramer: Produktivgenossenschaften als Instrument der Arbeitsmarktpolitik. Anmerkungen zum Berliner Förderungskonzept
- Heft 06/2003 Herbert Neunteufel/Gottfried Rössel/Uwe Sassenberg: Das Marketingniveau in der Kunststoffbranche Westmecklenburgs
- Heft 07/2003 Uwe Lämmel: Data-Mining mittels künstlicher neuronaler Netze
- Heft 08/2003 Harald Mumm: Entwurf und Implementierung einer objektorientierten Programmiersprache für die Paula-Virtuelle-Maschine
- Heft 09/2003 Jost W. Kramer: Optimaler Wettbewerb – Überlegungen zur Dimensionierung von Konkurrenz
- Heft 10/2003 Jost W. Kramer: The Allocation of Property Rights within Registered Co-operatives in Germany
- Heft 11/2003 Dietrich Nöthens/Ulrike Mauritz: IT-Sicherheit an der Hochschule Wismar
- Heft 12/2003 Stefan Wissuwa: Data Mining und XML. Modularisierung und Automatisierung von Verarbeitungsschritten
- Heft 13/2003 Bodo Wiegand-Hoffmeister: Optimierung der Sozialstaatlichkeit durch Grundrechtsschutz – Analyse neuerer Tendenzen der Rechtsprechung des Bundesverfassungsgerichts zu sozialen Implikationen der Grundrechte -
- Heft 14/2003 Todor Nenov Todorov: Wirtschaftswachstum und Effektivität der Industrieunternehmen beim Übergang zu einer Marktwirtschaft in Bulgarien
- Heft 15/2003 Robert Schediwy: Wien – Wismar – Weltkulturerbe. Grundlagen, Probleme und Perspektiven
- Heft 16/2003 Jost W. Kramer: Trends und Tendenzen der Genossenschaftsentwicklung in Deutschland
- Heft 01/2004 Uwe Lämmel: Der moderne Frege
- Heft 02/2004 Harald Mumm: Die Wirkungsweise von Betriebssystemen am Beispiel der Tastatur-Eingabe
- Heft 03/2004 Jost W. Kramer: Der Einsatz strategischer Planung in der Kirche
- Heft 04/2004 Uwe Sassenberg: Stand und Möglichkeiten zur Weiterentwicklung des Technologietransfers an der Hochschule Wismar
- Heft 05/2004 Thomas Gutteck: Umfrage zur Analyse der Kunden des Tourismuszentrum Mecklenburgische Ostseeküste GmbH
- Heft 06/2004: Anette Wilhelm: Probleme und Möglichkeiten zur Bestimmung der Promotioneffizienz bei konsumentengerichteten Promotions



- Heft 07/2004: Jana Otte: Personalistische Aktiengesellschaft  
Heft 08/2004: Andreas Strelow: VR-Control – Einführung eines verbundeinheitlichen Gesamtbanksteuerungskonzepts in einer kleinen Kreditgenossenschaft
- Heft 09/2004: Jost W. Kramer: Zur Eignung von Forschungsberichten als einem Instrument für die Messung der Forschungsaktivität
- Heft 10/2004: Jost W. Kramer: Geförderte Produktivgenossenschaften als Weg aus der Arbeitslosigkeit? Das Beispiel Berlin
- Heft 11/2004: Harald Mumm: Unterbrechungsgesteuerte Informationsverarbeitung
- Heft 12/2004: Jost W. Kramer: Besonderheiten beim Rating von Krankenhäusern
- Heft 01/2005: Michael Laske/Herbert Neunteufel: Vertrauen eine „Conditio sine qua non“ für Kooperationen?
- Heft 02/2005: Nicole Uhde: Rechtspraktische Probleme bei der Zwangseinziehung von GmbH-Geschäftsanteilen – Ein Beitrag zur Gestaltung von GmbH-Satzungen
- Heft 03/2005: Kathrin Kinder: Konzipierung und Einführung der Prozesskostenrechnung als eines Bestandteils des Qualitätsmanagements in der öffentlichen Verwaltung
- Heft 04/2005: Ralf Bernitt: Vergabeverfahren bei öffentlich (mit)finanzierten sozialen Dienstleistungen
- Heft 05/2005: Jost W. Kramer: Zur Forschungsaktivität von Professoren an Fachhochschulen am Beispiel der Hochschule Wismar
- Heft 06/2005: Harald Mumm: Der vollständige Aufbau eines einfachen Fahrradcomputers
- Heft 07/2005: Melanie Pippig: Risikomanagement im Krankenhaus
- Heft 08/2005: Yohanan Stryjan: The practice of social entrepreneurship: Theory and the Swedish experience
- Heft 09/2005: Sebastian Müller/Gerhard Müller: Sicherheits-orientiertes Portfoliomanagement
- Heft 10/2005: Jost W. Kramer: Internes Rating spezieller Kundensegmente bei den Banken in Mecklenburg-Vorpommern, unter besonderer Berücksichtigung von Nonprofit-Organisationen
- Heft 11/2005: Rolf Steding: Das Treuhandrecht und das Ende der Privatisierung in Ostdeutschland – Ein Rückblick –
- Heft 12/2005: Jost W. Kramer: Zur Prognose der Studierendenzahlen in Mecklenburg-Vorpommern bis 2020
- Heft 13/2005: Katrin Pampel: Anforderungen an ein betriebswirtschaftliches Risikomanagement unter Berücksichtigung nationaler und internationaler Prüfungsstandards