

**Florian Wiemken / Jan Markus Hempel**

**Corporate Governance und Sarbanes-Oxley  
Act - Haftungsrechtliche Anforderungen an  
die Unternehmensleitung und  
Risikomanagement von  
Aktiengesellschaften**

Unter besonderer Berücksichtigung der IT-Sicherheit

**Diplomarbeit**

## **Bibliografische Information der Deutschen Nationalbibliothek:**

Bibliografische Information der Deutschen Nationalbibliothek: Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de/> abrufbar.

Dieses Werk sowie alle darin enthaltenen einzelnen Beiträge und Abbildungen sind urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsschutz zugelassen ist, bedarf der vorherigen Zustimmung des Verlanges. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen, Auswertungen durch Datenbanken und für die Einspeicherung und Verarbeitung in elektronische Systeme. Alle Rechte, auch die des auszugsweisen Nachdrucks, der fotomechanischen Wiedergabe (einschließlich Mikrokopie) sowie der Auswertung durch Datenbanken oder ähnliche Einrichtungen, vorbehalten.

Copyright © 2005 Diplom.de  
ISBN: 9783832491703

**Florian Wiemken, Jan Markus Hempel**

**Corporate Governance und Sarbanes-Oxley Act - Haftungsrechtliche Anforderungen an die Unternehmensleitung und Risikomanagement von Aktiengesellschaften**

**Unter besonderer Berücksichtigung der IT-Sicherheit**



---

Florian Wiemken/Jan Markus Hempel

# Corporate Governance und Sarbanes-Oxley Act

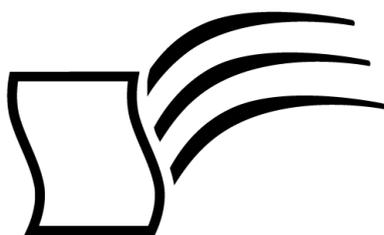
*Haftungsrechtliche Anforderungen an die Unternehmens-  
leitung und Risikomanagement von Aktiengesellschaften  
unter besonderer Berücksichtigung der IT-Sicherheit*

**Diplomarbeit**

**Carl-von-Ossietzky-Universität Oldenburg**

**Fachbereich Wirtschafts- und Rechtswissenschaften**

**Abgabe Oktober 2005**



***Diplom.de***

Diplomica GmbH \_\_\_\_\_  
Hermannstal 119k \_\_\_\_\_  
22119 Hamburg \_\_\_\_\_

Fon: 040 / 655 99 20 \_\_\_\_\_  
Fax: 040 / 655 99 222 \_\_\_\_\_

agentur@diplom.de \_\_\_\_\_  
www.diplom.de \_\_\_\_\_

ID 9170

Wiemken, Florian/Hempel, Jan Markus: Corporate Governance und Sarbanes-Oxley Act -  
Haftungsrechtliche Anforderungen an die Unternehmensleitung und Risikomanagement  
von Aktiengesellschaften unter besonderer Berücksichtigung der IT-Sicherheit  
Hamburg: Diplomica GmbH, 2006  
Zugl.: Carl-von-Ossietzky-Universität Oldenburg, Diplomarbeit, 2005

---

Dieses Werk ist urheberrechtlich geschützt. Die dadurch begründeten Rechte, insbesondere die der Übersetzung, des Nachdrucks, des Vortrags, der Entnahme von Abbildungen und Tabellen, der Funksendung, der Mikroverfilmung oder der Vervielfältigung auf anderen Wegen und der Speicherung in Datenverarbeitungsanlagen, bleiben, auch bei nur auszugsweiser Verwertung, vorbehalten. Eine Vervielfältigung dieses Werkes oder von Teilen dieses Werkes ist auch im Einzelfall nur in den Grenzen der gesetzlichen Bestimmungen des Urheberrechtsgesetzes der Bundesrepublik Deutschland in der jeweils geltenden Fassung zulässig. Sie ist grundsätzlich vergütungspflichtig. Zuwiderhandlungen unterliegen den Strafbestimmungen des Urheberrechtes.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Die Informationen in diesem Werk wurden mit Sorgfalt erarbeitet. Dennoch können Fehler nicht vollständig ausgeschlossen werden, und die Diplomarbeiten Agentur, die Autoren oder Übersetzer übernehmen keine juristische Verantwortung oder irgendeine Haftung für evtl. verbliebene fehlerhafte Angaben und deren Folgen.

Diplomica GmbH  
<http://www.diplom.de>, Hamburg 2006  
Printed in Germany

## Vita-Summary

### *Florian Wiemken*



Florian Wiemken studierte Diplom-Wirtschaftswissenschaften mit den Schwerpunkten Handels- und Wirtschaftsrecht, Rechnungswesen und Praktische Informatik an der Carl von Ossietzky Universität Oldenburg. Er verbrachte weiterhin drei Semester im Bachelor- und MBA-Programm an der University of Colorado at Denver und beschäftigte sich dort neben internationaler Rechnungslegung schwerpunktmäßig mit dem Management von Informationssystemen und Netzwerktechnik. Seine Diplomarbeit verfasste er zum Thema „Corporate Governance & Sarbanes-Oxley Act: Haftungsrechtliche Anforderungen und Risikovermeidungsstrategien für das Management von Aktiengesellschaften unter besonderer Berücksichtigung der IT-Sicherheit“ in Zusammenarbeit mit Jan Markus Hempel. Wiemken, der während des Studiums unter anderem für mehrere Wirtschaftsprüfungsgesellschaften tätig war, betreibt seit 1999 ein Einzelhandelsunternehmen und beschäftigt sich hierbei mit der Konzeption, dem Vertrieb und der Installation von IT-Hardwarelösungen für kleine und mittelständische Unternehmen. Gegenwärtig ist er im Bereich Assurance Business Advisory Services bei PricewaterhouseCoopers in Hamburg tätig.



## Florian Wiemken

Kanalstr. 28  
22085 Hamburg  
Tel.: 040 – 415 433 57  
Mobil: 0179 – 922 76 71  
eMail: Florian.Wiemken@web.de

geboren am 3. August 1979 in Oldenburg  
ledig

### Ausbildung

---

06/2003 bis 09/2005

#### **Carl von Ossietzky Universität Oldenburg**

*Diplomstudiengang Wirtschaftswissenschaften (Hauptstudium)*  
Schwerpunkte: Rechnungswesen, Internationales Wirtschaftsrecht,  
Praktische Informatik  
Abschluss: Diplom-Ökonom (voraussichtliche Note: 1,3)  
Diplomarbeit: „Corporate Governance & Sarbanes-Oxley Act:  
Haftungsrechtliche Anforderungen und Risikovermeidungsstrategien für  
die Unternehmensleitung im Hinblick auf die IT-Sicherheit“

08/2002 bis 05/2003,  
08/2004 bis 12/2004

#### **University of Colorado at Denver, USA**

*Faculty of Business and Computer Science*  
Drei Austauschsemester im BS- und MBA-Programm  
GPA: 4,0/4,0

08/2000 bis 07/2002

#### **Carl von Ossietzky Universität Oldenburg**

*Diplomstudiengang Wirtschaftswissenschaften (Grundstudium)*  
Abschluss: Vordiplom (Note 1,6)

08/1992 bis 07/1999

#### **Gymnasium der KGS Rastede**

Prüfungsfächer: Englisch, Chemie, Französisch, Politik  
Abschluss: Abitur (Note 1,7)

### Praktika und unternehmerische Tätigkeit

---

10/2003 bis 02/2004

#### **PricewaterhouseCoopers (PwC) Deutsche Revision AG**

*Frankfurt am Main*  
Bereich: Wirtschaftsprüfung und prüfungsnaher Dienstleistungen  
Tätigkeiten: Prüfung verschiedenster Bilanzpositionen großer und  
mittelgroßer Kapitalgesellschaften nach deutschen und internationalen  
Rechnungslegungsvorschriften

01/2003 bis 05/2003

#### **University of Colorado at Denver**

*Denver, Colorado, USA* *(studienbegleitend)*  
Bereich: Marketing-Assistent im Office of International Education  
Tätigkeiten: Vermarktung internationaler Austauschprogramme unter  
12.000 Studierenden, Präsentationen, Organisation und Durchführung  
einer Hochschulmesse, Beratung und Rekrutierung

...weitere auf Seite 2...

- 03/2002 bis 04/2002      **Treuhand Oldenburg und Partner OHG**  
*Oldenburg*  
 Bereich: Wirtschaftsprüfung und Steuerberatung  
 Tätigkeiten: Jahresabschlussprüfung einer großen Kapitalgesellschaft des Baugewerbes, Erstellung kleinerer Jahresabschlüsse und Steuererklärungen, Literaturrecherchen
- 12/2000 bis 07/2001      **Canbox Systems AG & Canbox Dialog GmbH**  
*Oldenburg*      *(studienbegleitend)*  
 Bereich: Customer Care Support  
 Tätigkeiten: europaweite Betreuung von Endkunden verschiedener Freemail-Anbieter, Mitarbeit am Aufbau eines Online-Supportsystems
- 01/1999 bis heute      **Gründung des Einzelunternehmens FW-Computer**  
*Oldenburg*      *(studienbegleitend)*  
 Tätigkeit: Einzelhandel mit EDV-Hardware und Telekommunikationsprodukten, Service, Beratung, Schulung.  
 Kundenkreis: mittelständische Unternehmen, Privatkunden

### Zivildienst

- 07/1999 bis 07/2000      **Evang.-Luth. Kirchengemeinde Oldenburg**  
*Verwaltung*

### Aktivitäten

- 05/2002      Jahresstipendiat der Floyd und Lili Biava-Stiftung
- 02/2002 bis 07/2002      Offizieller Betreuer und Ansprechpartner für amerikanische Austauschstudenten an der Universität Oldenburg
- 11/2001 bis 07/2002      Planung, Organisation und Durchführung des Hochschulballs der Universität Oldenburg in einem studentischen Team, persönliche Verantwortung für 20.000,- EUR Budget und 800 Gäste
- 04/2001 bis 08/2002      Mitgründer und Vorstandsmitglied  
 „Campus & Company e.V.“

### Sprachkenntnisse

Englisch (verhandlungssicher), Französisch (konversationsfähig), Spanisch (Grundkenntnisse)

### EDV-Kenntnisse

MS-Officepaket, Lotus Notes (sehr gut), SAP/R3 FI (Grundkenntnisse), Netzwerke, Architekturen, Hardware, Webdesign, C# (fortgeschritten)

### Hobbys / Interessen

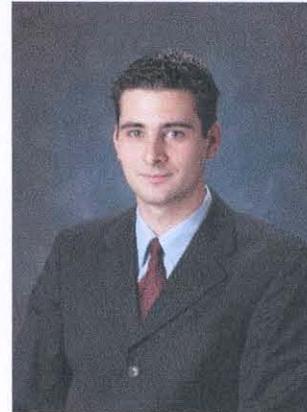
Organisieren, Reisen, Computer, Lesen, Skifahren, Motorradfahren

Hamburg, 12.12.2005

*Florian Wiemken*

## Vita-Summary

### *Markus Hempel*



Jan Markus Hempel studierte Wirtschaftswissenschaften mit Schwerpunkt Informatik und Betriebswirtschaftslehre mit juristischem Schwerpunkt an der Carl von Ossietzky Universität Oldenburg. Zudem hat er ein zweijähriges Studium an der Universität Le Havre mit einem Master in Außenhandel und Internationalen Finanzen abgeschlossen. An der University of Colorado at Denver verbrachte Jan Markus Hempel ein zusätzliches Studienjahr mit den Schwerpunkten Strategisches Management und Informationssysteme, in dessen Rahmen er ein Disaster Recovery Planning Projekt für Qwest Telecom begleitete. Nach seiner Abschlussarbeit zum Thema „The Sarbanes - Oxley Act Section 404 and the implication on IT“ bei DaimlerChrysler Services ist eine weitere Diplomarbeit mit haftungsrechtlichem Schwerpunkt in Kooperation mit Florian Wiemken in Arbeit.

Herr Hempel berät seit 2002 deutsche Unternehmen beim Markteintritt in Frankreich und ist seit 2004 in Paris als Berater und Auditor im IT - Riskmanagement bei PricewaterhouseCoopers tätig.

## LEBENS LAUF

### Jan Markus Hempel

55 avenue Puvis De Chavannes  
92400 Courbevoie/ Frankreich  
Telefon: 0033 621 46 52 14  
Email: [markus.hempel@web.de](mailto:markus.hempel@web.de)



#### ■ Persönliche Daten

Familienstand: ledig  
Staatsangehörigkeit: deutsch  
Geburtsdaten: 9. Juni 1977 in Bergen auf der Insel Rügen

#### ■ Studium und Schulbildung

November 2004 **Diplom Wirtschaftswissenschaften mit Schwerpunkt Informatik** (Abschlussnote: 1,52) und **Diplom BWL mit juristischem Schwerpunkt** (vor. Abschluss Nov. 2005: gut) an der Carl von Ossietzky Universität Oldenburg. Studienschwerpunkte: Strategisches Management, Projektmanagement, Informationssysteme, Europarecht

08/2002 – 06/2003 Studium in **Management und Informatik** an der **University of Colorado at Denver, USA**, GPA 3,84 /4

09/2000 – 06/2002 **Diplom „Außenhandel und Internationale Finanzen“** an der **Universität Le Havre, Frankreich** (Doppeldiplom) und **franz. Vordiplom**

10/1998 – 07/2000 **Vordiplom** in BWL und Wirtschaftswissenschaften an der Carl von Ossietzky Universität Oldenburg

06/1997 **Abitur**, Prüfungsfächer: Englisch, Deutsch, Mathematik, GK  
07/1989 – 06/1997 Gymnasien in Berlin, Triberg (Schwarzwald) u. Hameln  
06/1984 – 06/1989 Grundschule in Bergen auf Rügen

#### ■ Praktische Erfahrungen

10/2004 – aktuell IT – Consultant/ Auditor, **PricewaterhouseCoopers, Paris**, Bereich Systems & Process Assurance, *Projekte:* Sarbanes – Oxley Act 404 Compliance, IT-Systemprüfung, SAP Reviews

03/2004 – 08/2004 Praxis-Diplomarbeit „The Sarbanes-Oxley Act 404 - The implication on IT“ bei der **DaimlerChrysler Services AG, Stuttgart** und Projektarbeit für SOA 404 in europäischen Filialen, Bereich IT - Management; Note:1,0.

09/2003 – 01/2004 Praktikum bei **PricewaterhouseCoopers, Paris**, Bereich „Operational and Systems Risk Management“, *Projekte:* Sarbanes – Oxley Act 404 Compliance, Data Management, IT-Systemprüfung

03/2002 – 10/2004 Gründung des studentischen Unternehmens **ASPECT International Business Services**, Internationale Vertriebsberatung für Deutschland, Frankreich und GB in den Bereichen IT, Logistik und Telekom; *Aktivitäten:* Vertriebspartnersuche, Partnerschulung, Repräsentation, Verhandlungsführung mit den Partnern, Vorträge zu SOX.

02/2002 – 05/2002	Praktikum bei der Kommunikationsagentur <b>DBcom, in Le Havre, Frankreich</b> <i>Aktivitäten:</i> Kommunikationsberatung, Anzeigenverkauf
06/2001 – 09/2001	Praktikum bei <b>PricewaterhouseCoopers, Frankfurt am Main</b> , Bereich „Global Risk Management Solutions“, prüfungsnaher IT-Beratung; <i>Projekte:</i> Due Dilligence, IT- Prüfungen, Prozessoptimierung, Data Management
05/2000 – 09/2000	Praktikum bei <b>Tecis Finanzdienstleistungen, Oldenburg</b> ; <i>Aktivitäten:</i> Anlageberatung für Privatkunden, Fondsvertrieb
08/1997 – 08/1998	<b>Zivildienst, Technischer Dienst</b> im Seniorenheim St. Monika, Hameln; <i>Aktivitäten:</i> Verwaltung, Pflege

### ■ Auslandsaufenthalte

07/2003 – 02/2004	Praktikum und Kundenprojekte in <b>Paris, Frankreich</b>
08/2002 – 06/2003	Studium an der University of Colorado at <b>Denver, USA</b>
09/2000 – 07/2002	Diplomstudium an der Université <b>Le Havre, Frankreich</b>

### ■ Sprachkenntnisse

**Englisch:** fließend in Wort und Schrift  
**Französisch:** fließend in Wort und Schrift  
**Spanisch:** Gute Kenntnisse, Intensivkurs Okt. 2004

### ■ IT- Kenntnisse

**Programme und Systeme:** Alle Windowssysteme, Word, Excel, PowerPoint, Access, MS Project, MS Visio, MicroStrategy7 (Datamining), Lotus Notes, Frontpage, VoIP - Telefonie, Kenntnisse SAP R/3 (SD, MM, FI/CO);  
**Programmierung:** Basiskenntnisse in SQL, ACL, HTML

### ■ Zertifikate

**D.E.L.F., 1er degré:** Offizielles Sprachdiplom des französischen Bildungsministeriums  
**Certified Data Warehouse Engineer,** MicroStrategy

### ■ Stipendien

**Stipendium M.I.L.C.** der Region Haute-Normandie

### ■ Sonstige Aktivitäten

Seit 04/1999	Aktives Mitglied der <b>Studentenorganisation MARKET TEAM</b> , <i>Projekte:</i> Organisation eines Firmenforums für 20 Unternehmen und ca. 2000 Studenten
--------------	--

### ■ Referenzen

Beruflich :	Auf Anfrage.
Akademisch :	Prof. Dr. Jürgen Taeger, Direktor des Instituts für Rechtswissenschaften an der Universität Oldenburg, Tel. : 0441 798 4136

Paris, 15. Oktober 2005



Markus Hempel

# INHALT

DARSTELLUNGSVERZEICHNIS .....	V
ABKÜRZUNGSVERZEICHNIS.....	VII
I. MANAGER UND IHR BERUFSRISIKO .....	1
II. GRUNDLAGEN DER ORGANHAFTUNG.....	5
A. Einführende Grundbegriffe.....	5
1. Definition und Abgrenzung.....	5
2. Szenarien der Haftung .....	7
3. Kreis der Haftpflichtigen und Anspruchsberechtigten.....	7
B. Innenhaftung .....	8
1. Vorstände.....	9
2. Aufsichtsräte.....	22
3. Haftungsbeschränkung .....	29
C. Außenhaftung.....	30
1. Deliktische Schadensersatzansprüche.....	31
2. Regressansprüche .....	33
3. Haftung gegenüber den verschiedenen Anspruchstellern.....	34
III. CORPORATE GOVERNANCE: ORGANHAFTUNG IM WANDEL .....	47
A. Die Corporate Governance-Diskussion in Deutschland .....	48
1. Hintergründe.....	48
2. Vorstellungen von Corporate Governance .....	53
B. Das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) ..	55
1. Zielsetzung .....	55
2. Erweiterung der Berichtspflichten des Vorstands (§ 90 Abs. 1 Nr. 1 AktG).....	56
3. Risikomanagement und interne Kontrolle (§ 91 Abs. 2 AktG) .....	58
4. Geltendmachung von Ersatzansprüchen durch Minderheitsverlangen (§ 147 AktG).....	67
5. Mittelbare Auswirkungen des KonTraG auf die Managerhaftung .....	68
6. Zusammenfassung und abschließende Kritik .....	69
C. Der Deutsche Corporate Governance Kodex (DCGK).....	70
1. Entwicklung des DCGK .....	70
2. Wirkungsweise des DCGK.....	73
3. Ausgewählte materielle Klarstellungen und Neuregelungen durch den DCGK.....	75
4. Durchsetzbarkeit und Haftungsrisiken aus dem DCGK .....	84
5. Kritische Würdigung des DCGK.....	91

D. Das Transparenz- und Publizitätsgesetz (TransPuG).....	93
1. Das TransPuG als zweite Umsetzungsstufe.....	93
2. Intensivierung der Berichtspflichten (§ 90 Abs. 1 AktG).....	94
3. Obligatorische Zustimmungsvorbehalte des Aufsichtsrats (§ 111 Abs. 4 AktG).....	94
4. Erweiterung der Prüfung des Risikofrüherkennungssystems (§ 317 Abs. 4 HGB).....	94
E. Das Vierte Finanzmarktförderungsgesetz.....	95
1. Stärkung des Finanzplatzes Deutschland.....	95
2. Kodifizierung von Schadensersatzansprüchen (§§ 37b, 37c WpHG).....	96
F. Das 10-Punkte-Programm „Unternehmensintegrität und Anlegerschutz“.....	98
1. Das Programm als dritte Umsetzungsstufe.....	98
2. Verbesserung des Klagerechts der Aktionäre und „Business Judgment Rule“ (UMAG)..	99
3. „Enforcement“ zur Überwachung der Unternehmensabschlüsse (BilKoG).....	102
4. Erweiterung der zukunftsorientierten Lageberichterstattung (BilReG).....	103
5. Persönliche Haftung für Falschinformationen des Kapitalmarkts (AnsVG, KapInHaG, KapMuG).....	105
 IV. DER SARBANES – OXLEY ACT OF 2002.....	 110
A. Vorstellung des Sarbanes - Oxley Act (SOA).....	111
1. Hintergründe und Ziele.....	111
2. Inhalte und Bestimmungen des Gesetzes.....	113
3. Wirkungsbereich des Gesetzes.....	116
B. Auswirkungen des SOA auf die Unternehmen.....	119
1. Vorstandshaftung und Anforderungen an das Management.....	119
2. Corporate Governance und Ethikdiskussion im Kontext des SOA.....	122
3. Verstärkung des internen Kontrollsystems.....	125
C. Kritische Würdigung des SOA.....	132
1. Zwischenbilanz des SOA.....	132
2. SOA als Kostenfaktor.....	134
3. Chancen der SOA Konformität.....	137
 V. IT-RISIKEN UND IT-SICHERHEIT.....	 140
A. Technische Anforderungen an die IT-Sicherheit.....	143
1. Begriffliche Grundlagen der IT-Sicherheit.....	143
2. Gefahren für die IT-Sicherheit.....	145
3. Gefährdungsebenen und Sicherheitsaspekte.....	147
4. Sicherheits- und Katastrophenmanagement.....	152
B. Rechtliche Anforderungen an die IT-Sicherheit.....	153
1. Im weiteren Sinn aus dem Aktiengesetz.....	154
2. Im engeren Sinn aus datenschutzrelevanten Gesetzen.....	155
3. Grundsätze ordnungsgemäßer Datenverarbeitung im Rechnungswesen.....	160
C. Verantwortung für die Umsetzung der Anforderungen.....	162

VI. RISIKOMANAGEMENT UND DIE ROLLE DER IT .....	164
A. Ausgestaltung eines Risikomanagementsystems .....	165
1. Einführung eines Risikomanagementsystems.....	165
2. Risikomanagement nach dem COSO II Standard.....	178
3. Die Auswirkungen von Basel II auf das Risikomanagement .....	180
4. Kritische Würdigung des Risikomanagements.....	184
B. Integration der IT in das Risikomanagement .....	186
1. Unterstützung des Risikomanagements durch die IT .....	186
2. Bewältigung von IT-Risiken durch IT-Governance .....	190
VII. STRATEGIEN ZUR RISIKOBEWÄLTIGUNG .....	194
A. Best - Practice Strategien in der IT .....	194
1. Einführung der IT Governance am Beispiel des COBIT .....	194
2. Konsolidierung des COBIT mit dem COSO Standard .....	199
B. Sonstige Risikovermeidungsstrategien .....	200
1. D&O – Versicherungen .....	200
2. Dokumentation der Entscheidungsfindung.....	201
3. Outsourcing .....	201
VIII. ZUSAMMENFASSUNG UND AUSBLICK.....	202
LITERATUR .....	205
WEBQUELLEN.....	216

## Darstellungsverzeichnis

Darstellung 1:	Managerhaftung im Überblick
Darstellung 2:	Verpflichtungen des Managements aus dem SOA
Darstellung 3:	Weitere Verpflichtungen des Managements aus dem SOA
Darstellung 4:	Die Bedeutung der Section 404 für das IKS
Darstellung 5:	Das interne Kontrollsystem und seine Regelungsbereiche
Darstellung 6:	Das integrierte COSO Rahmenwerk (COSO I Würfel)
Darstellung 7:	IDW Version des COSO Rahmenwerks
Darstellung 8:	Methodik zur Umsetzung von IKS / 302 / 404 Projekten
Darstellung 9:	Bestimmung der Konformitätskosten
Darstellung 10:	Kontinuierliche Compliance und Verbesserung
Darstellung 11:	Kategorien von Gefahren für die IS-Sicherheit
Darstellung 12:	Gefahren im Schnittpunkt von Gefährdungsebenen und Sicherheitsaspekten
Darstellung 13:	Verletzung der Vertraulichkeit
Darstellung 14:	Verletzung der Integrität
Darstellung 15:	Verletzung der Verfügbarkeit
Darstellung 16:	Verletzung der Verbindlichkeit
Darstellung 17:	Der Sicherheitskubus
Darstellung 18:	Übersicht der datenschutzrelevanten Vorschriften in Rechnernetzen
Darstellung 19:	Acht Gebote der Datensicherheit nach Anlage zu § 9 BDSG
Darstellung 20:	Prozessstruktur des Risikomanagements
Darstellung 21:	Prozessuale Sicht des Risikomanagements
Darstellung 22:	Beispiel für eine Risikokategorisierung
Darstellung 23:	Prozessdarstellung des Unternehmens zur Identifikation von Risiken
Darstellung 24:	Beispiel für ein Risikoportfolio
Darstellung 25:	Prozess der Risikosteuerung und -Kontrolle
Darstellung 26:	COSO II Modell mit ERM
Darstellung 27:	Drei-Säulen-Modell der Basel II Vereinbarung
Darstellung 28:	Regulatorischer Ansatz bei MaRisk und Basel II
Darstellung 29:	Datenaufbereitung von relevanten Managementinformationen
Darstellung 30:	Funktionsweise der IT-Governance
Darstellung 31:	Risikoanalyse auf der Basis von IT-Grundschutz

Darstellung 32:	Kriterien für Qualität, Sicherheit und Ordnungsmäßigkeit aus COBIT
Darstellung 33:	IT-Ressourcen und ihre Bedeutung für das COBIT
Darstellung 34:	Die inneren Zusammenhänge des COBIT-Modells
Darstellung 35:	Die internen Kontrollebenen der Finanzberichterstattung
Darstellung 36:	COSO / COBIT Kombination

## Abkürzungsverzeichnis

a.F.	alte Fassung
AICPA	American Institute of Certified Public Accountants
AktG	Aktiengesetz
AMEX	American Stock and Options Exchange
AnSVG	Anlegerschutzverbesserungsgesetz
AO	Abgabenordnung
B2B	Business-to-Business
B2C	Business-to-Consumer
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BilKoG	Bilanzkontrollgesetz
BilReG	Bilanzrechtsreformgesetz
BS	British Standard
BSC	Balanced Scorecard
CEAC	Compagnie européenne d'accumulateurs
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CNIL	Commission nationale de l'informatique et des libertés
COBIT	Control Objectives for Information and related Technology
COSO	Committee of Sponsoring Organizations of the Treadway Commission
DCGK	Deutscher Corporate Governance Kodex
D&O	Director's and Officer's Liability Insurance
DV	Datenverarbeitung
EDV	Elektronische Datenverarbeitung
ERM	Enterprise Risk Management
ERP	Enterprise Resource Planning
FPI	Foreign Private Issuer
GAAP	Generally Accepted Accounting Principles
GCCG	German Code of Corporate Governance
GoB	Grundsätze ordnungsgemäßer Buchführung
HGB	Handelsgesetzbuch
H.M.	Herrschende Meinung
HW	Hardware
IDW	Institut der Wirtschaftsprüfer in Deutschland e.V.
IKS	Internes Kontrollsystem
InsO	Insolvenzordnung
IS	Informationssystem

ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
IT	Informationstechnologie
ITGI	IT Governance Institute
ITIL	Information Technology Infrastructure Library
IuK	Information- und Kommunikation
KapInHaG	Kapitalmarktinformationshaftungsgesetz
KapMuG	Kapitalanlegermusterverfahrensgesetz
KonTraG	Kontroll- und Transparenzgesetz
MaRisk	Mindestanforderungen an das Risikomanagement
MG	Metallgesellschaft AG
MW	Manware
NASDAQ	National Association of Securities Dealers Automated Quotations
n.F.	neue Fassung
NYSE	New York Stock Exchange
OECD	Organization for Economic Cooperation and Development
OW	Orgware
PCAOB	Public Company Accounting Oversight Board
PS	Prüfungsstandard
PwC	PricewaterhouseCoopers
RMIS	Risikomanagement-Informationssystem
SAS	Statement of Auditing Standard
SEC	Securities Exchange Commission
SLA	Service Level Agreement
SOA	Sarbanes - Oxley Act
SOX	Sarbanes - Oxley Act
StGB	Strafgesetzbuch
SW	Software
TransPuG	Transparenz - und Publizitätsgesetz
UMAG	Gesetz zur Unternehmensintegrität und Modernisierung des Anfechtungsrechts
US	United States
VaR	Value-at-Risk
WpHG	Wertpapierhandelsgesetz

## I. Manager und ihr Berufsrisiko

Vorstände von Aktiengesellschaften agieren als Treuhänder fremden Vermögens. Um Anleger und Gläubiger zu schützen haben sie bei ihrem Handeln und der Organisation des Unternehmens bestimmte gesetzliche Vorschriften zu beachten. Jedoch beschäftigten sich bis Mitte der neunziger Jahre weder das Schrifttum noch die Rechtsprechung wesentlich mit der Frage der persönlichen Haftung der Vorstandsmitglieder für Fehlentscheidungen oder Pflichtverletzungen.<sup>1</sup> Eine Pflichtverletzung, die zu einem Schaden bei der Gesellschaft führte, wurde in der Regel lediglich personalpolitisch sanktioniert.<sup>2</sup> Die betroffenen Unternehmen sahen dabei zumindest dann von der Geltendmachung weiterer Ansprüche wie Schadenersatz oder der Strafanzeige ab, sofern der Verantwortliche keine unakzeptablen Abfindungsforderungen stellte. Verständlicherweise stehen vor allem die Vorstandsmitglieder selbst weitergehenden Forderungen kritisch gegenüber und verweisen auf eine Einschränkung der unternehmerischen Freiheit.<sup>3</sup> Allerdings lassen sich auch im juristischen Schrifttum Stimmen finden, die personalpolitische Konsequenzen als „im Großen und Ganzen“ ausreichend ansahen.<sup>4</sup>

Beginnend in der zweiten Hälfte der neunziger Jahre setzte dann allerdings eine schnell an Fahrt gewinnende Bewegung ein. Die zahlreichen Bilanzierungsskandale und Unternehmenszusammenbrüche in jüngerer Zeit haben etlichen Anlegern große Verluste beschert und insgesamt das Vertrauen in die weltweiten Kapitalmärkte empfindlich erschüttert. Hinzu kam, dass international vergleichbare Standards für die Verantwortung der Unternehmensleitung fehlten, obwohl die Unternehmen durch die Globalisierung der Märkte zunehmend international verflochten sind.<sup>5</sup>

Um diesen Entwicklungen entgegenzuwirken haben Gesetzgeber und Börsenaufsichtsbehörden erhebliche Anstrengungen in Form von neuen Gesetzen und Vorschriften unternommen. Gesetzgebung und Rechtsprechung haben die Haftungsvoraussetzungen nicht nur konkretisiert, sondern vor allem auch zu Lasten der Unternehmensleitung verschärft.<sup>6</sup>

Bei vielen Unternehmensinsolvenzen stellte sich im nachhinein heraus, dass die Krise absehbar und abwendbar gewesen wäre, wenn die Aufsichtsratsmitglieder ihre Überwachungsaufgabe gewissenhaft wahrgenommen hätten. Aus diesem Grund ist auch die Haftung des Aufsichtsrats der Aktiengesellschaft in den Blickpunkt der öffentlichen Diskussion geraten.

---

<sup>1</sup> Vgl. *Thümmel*, Haftung von Managern, 2003, Rn. 1.

<sup>2</sup> Entweder wurde der betreffende Vorstand gemäß § 84 Abs. 1 AktG nicht wiederbestellt oder, bei schwerwiegenden Fällen, nach § 84 Abs. 3 AktG vorzeitig abberufen. Vgl. *Horn*, ZIP 1997, S. 1129 (1130).

<sup>3</sup> Siehe *Schaudwet*, WiWo 41/04, S. 47.

<sup>4</sup> So zum Beispiel *Horn*, ZIP 1997, S. 1129 (1130).

<sup>5</sup> Siehe *Thümmel*, Haftung von Managern, 2003, Rn. 3.

<sup>6</sup> Vgl. *Sieg*, DB 2002, S. 1759.

Die nach wie vor andauernden Aktivitäten des Gesetzgebers sind Teil der international geführten Diskussion um Standards guter Unternehmensführung und Unternehmenskontrolle (Corporate Governance). Die Diskussion hat ausgehend von den USA mittlerweile auch Europa und Deutschland erfasst. Auffällig hierbei ist die Tendenz, neben der Gesellschaft als juristischer Person auch die Organmitglieder selbst zivil- und strafrechtlich in Haftung nehmen zu wollen, wenn sie ihre Sorgfaltspflichten verletzt haben. Die Haftung der Unternehmensleitung hat damit komplexere und vor allem für die betroffenen Vorstands- und Aufsichtsratsmitglieder immer schwieriger zu überblickende Ausmaße angenommen. Obwohl die Preise spezieller Haftpflichtpolice in jüngster Zeit explodiert sind und hohe Selbstbeteiligungen vorsehen, sind sich viele Vorstände und Aufsichtsräte ihrer Pflichten und der Haftungsrisiken, die sie durch ihre Funktion in der Gesellschaft persönlich treffen, nicht hinreichend bewusst.

Vor diesem Hintergrund stellt die vorliegende Arbeit im zweiten Kapitel zunächst die Struktur, Systematik und wichtigsten Tatbestände der Organhaftung der Aktiengesellschaft dar. Hiermit wird die Grundlage für das Verständnis der im Zuge der Corporate Governance-Diskussion entstandenen neueren Entwicklungen gelegt.

Eines der Hauptanliegen der Corporate Governance-Bewegung ist es, wirksame Mittel und Anreize zu finden, weitere Fälle von Missmanagement in Zukunft zu verhindern. Die Einführung und Durchsetzung der persönlichen Haftung der Organmitglieder kann dabei aber lediglich *eines* der Instrumente sein, um sicherzustellen, dass Vorstands- und Aufsichtsratsmitglieder ihre Funktion ordnungsgemäß wahrnehmen. Das zweite wesentliche Element präventiver Art ist ein effektives, in der eigenen Unternehmenskultur verankertes internes Kontrollsystem, das Schwachstellen verhindert oder zumindest frühzeitig erkennt und es den Verantwortlichen ermöglicht, noch rechtzeitig Gegenmaßnahmen einzuleiten. So verpflichtet das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) den Vorstand von Aktiengesellschaften „geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden“.<sup>7</sup>

Bestandsgefährdend kann für ein Unternehmen eine Vielzahl ganz unterschiedlicher Entwicklungen sein. Auch können sich einzelne Risiken durch gegenseitige Wechselwirkungen erst zu bestandsgefährdenden Entwicklungen ausbilden. Im Schrifttum wird daher immer wieder gefordert, das Überwachungssystem in ein unternehmensweites Risikomanagementsystem einzubetten. Unklar und umstritten ist hierbei allerdings, wie ein solches Risikomanagementsystem ausgestaltet sein muss, da das Gesetz hierzu keine konkreten Angaben macht. Eine genaue Vorstellung der gesetzlichen Anforderungen ist jedoch entscheidend für die Organmitglieder, um sich nicht selbst wegen einer Sorgfaltspflichtverletzung durch Unterlassen haftbar zu machen. Aus diesem Grund stellt die Arbeit im dritten Kapitel

---

<sup>7</sup> § 91 Abs. 2 AktG.

die relevanten neueren Gesetze, die in den vergangenen zehn Jahren im Rahmen der Corporate Governance-Diskussion entstanden sind, vor. Ziel der Untersuchung ist es, die Pflicht zur Einrichtung eines Risikomanagementsystems herauszuarbeiten und Anhaltspunkte für dessen Ausgestaltung zu finden. Durch eine chronologische Darstellung, die die einzelnen Gesetzesinitiativen jeweils in den Gesamtkontext der Diskussion um Corporate Governance einordnet, soll außerdem gezeigt werden, mit welcher Dynamik sich die persönliche Haftungssituation der Organmitglieder mittlerweile verändert und welche Rolle hierbei dem Risikomanagement zukommt.

Wesentliche Impulse und Anregungen für die Weiterentwicklung des deutschen Modells der Unternehmenskontrolle kamen mit dem US-amerikanischen Sarbanes-Oxley Act, der deshalb anschließend im vierten Kapitel vorgestellt wird. Der Sarbanes-Oxley Act verpflichtet auch deutsche Unternehmen, die an US-Börsen notiert sind, für nach dem 15. Juli 2006 endende Geschäftsjahre ein internes Kontrollsystem über die Finanzberichterstattung einzuführen, dieses zu dokumentieren und die Wirksamkeit jährlich von Abschlussprüfern testieren zu lassen.<sup>8</sup> Weiterhin sind Chief Executive Officer (CEO) und Chief Financial Officer (CFO) eines Unternehmens verpflichtet, den Jahresabschluss und sonstige Berichte der Gesellschaft persönlich zu zertifizieren. Die Bestätigung der Korrektheit bezieht sich dabei auch auf das Vorhandensein sowie die Effektivität interner Kontrollmechanismen und wird durch die Androhung von bis zu 20 Jahren Gefängnis strafrechtlich flankiert.<sup>9</sup>

Im weiteren Verlauf zeigt die Arbeit auf, wie ein Risikomanagementsystem, welches den haftungsrechtlichen Anforderungen gerecht wird, im Unternehmen umgesetzt werden kann. Hierzu werden Best Practise-Standards und Referenzmodelle vorgestellt. Der Fokus soll dabei konkret auf den Umgang mit Risiken gelegt werden, die sich aus dem Einsatz von unternehmensweiten Informationssystemen und deren Technologie ergeben. Hierfür gibt es vier Gründe.

Erstens ist wirtschaftlicher Erfolg von Unternehmen heute mehr denn je auf zuverlässige und sichere Informationstechnologie (IT) angewiesen, da die Geschäftsprozesse über vernetzte IT-Systeme ausgeführt und abgebildet werden. Die Wettbewerbsvorteile, die sich mit dem effizienten Einsatz von IT erzielen lassen, haben allerdings einen Preis: Die Sicherheit der IT-Systeme ist ein wachsendes Risiko und eine Schwachstelle für viele Unternehmen. Die Auswirkungen von Störungen oder Angriffen auf ein Informationssystem sind nicht nur in finanziellen Verlusten zu sehen – sie können unter Umständen sogar den Fortbestand des gesamten Unternehmens bedrohen.

Zweitens wird auch der überwiegende Teil der im Unternehmen einzurichtenden internen Kontrollmechanismen in automatisierter Form in der Unternehmenssoftware

---

<sup>8</sup> Siehe *Hempel*, *Implication on IT*, 2004, S. VI.

<sup>9</sup> Siehe *Kersting*, *ZIP* 2003, S. 233.

zu implementieren sein. Die IT-Sicherheit ist daher Voraussetzung für die Wirksamkeit und Verlässlichkeit dieser Kontrollmechanismen.

Drittens hängt auch die Finanzberichterstattung des Hauses entscheidend von einem ordnungsgemäß funktionierenden Informations- und Kontrollsystem ab, da die Geschäftsvorgänge elektronisch erfasst werden und diese Daten dann dem internen und externen Rechnungswesen zugrunde liegen. Insbesondere für kapitalmarktorientierte Aktiengesellschaften stellen sowohl der Sarbanes-Oxley Act wie auch die deutschen Gesetze besonders hohe Anforderungen an die Richtigkeit der Finanzberichterstattung. Neben den direkten, inhärenten Risiken aus dem Einsatz von IT ergeben sich daher weitere indirekte Risiken für Vorstände und Aufsichtsräte bei der Finanzberichterstattung.

Schließlich ist die IT-Sicherheit auch ein Bestandteil bei der Bestimmung der Kreditwürdigkeit eines Unternehmens. So fordert die neue Baseler Eigenkapitalvereinbarung („Basel II“) die Offenlegung operationeller IT-Risiken und deren Unterlegung mit Eigenkapital.

Das persönliche Interesse der Verfasser an dem IT-Schwerpunkt ergab sich aus dem Wunsch, ein Thema im Schnittpunkt von Wirtschaftswissenschaften, Rechtswissenschaften und Informatik zu bearbeiten, da dieses individuelle Studienschwerpunkte beider Verfasser waren. Nach ihrer Auffassung bestehen nach wie vor Kommunikations- und Verständnisprobleme zwischen Wirtschaftswissenschaftlern, Juristen und Informatikern, die sich aus unterschiedlichen Denkweisen begründen. Die Motivation liegt daher darin, die verschiedenen Facetten in einer interdisziplinären Arbeit zu beleuchten, da sich nur so ein ganzheitlicher Blick auf die Thematik eröffnet. Die IT-Sicherheit ist als ein Kernstück des unternehmenseigenen Risikomanagements zu sehen, was wiederum zentrale Bedeutung für die Finanzberichterstattung hat, von dessen Richtigkeit das Funktionieren der weltweiten Kapitalmärkte und damit letztlich ein wesentlicher Teil der Volkswirtschaft abhängt.

Vor diesem Hintergrund setzt die Arbeit im fünften Kapitel fort mit einer kurzen Darstellung der Anforderungen an die IT-Sicherheit aus technischer und rechtlicher Sicht. Anschließend wird im sechsten und siebten Kapitel gezeigt, wie der Umgang mit IT-Risiken in ein unternehmensweites Risikomanagementsystem gesetzeskonform eingebunden werden kann und welche weiteren Risikovermeidungsstrategien den Organmitgliedern zur Verfügung stehen.

Im Zentrum der juristischen Betrachtung steht die Aktiengesellschaft, da die Diskussion um Corporate Governance von den Anforderungen des Kapitalmarkts getrieben wird und auf diesen ausgerichtet ist. Die Aktiengesellschaft spielt deshalb eine Vorreiterrolle im Fokus der Gesetzesinitiativen auch für andere Rechtsformen. Vor allem die (Gesellschafter-)Geschäftsführer von GmbH bzw. GmbH & Co. KG sollten sich mit den haftungsrechtlichen Anforderungen an ihre AG-Kollegen auseinandersetzen, da von einer Ausstrahlungswirkung auch auf diese Kapitalgesellschaften auszugehen ist.

## II. Grundlagen der Organhaftung

### A. Einführende Grundbegriffe

#### 1. Definition und Abgrenzung

Die Aktiengesellschaft hat drei Organe: Vorstand, Aufsichtsrat und Hauptversammlung. Die noch zu behandelnden Organfunktionen werden von den Organmitgliedern wahrgenommen. Vorstand und Aufsichtsrat setzen sich im Regelfall aus mehreren Personen zusammen, die durch einen Dienstvertrag angestellt sind, während die Hauptversammlung aus Aktionären gebildet wird.

Mit dem Begriff der Organhaftung wird die Verpflichtung des Organmitglieds begründet, für von ihm durch Tun oder Unterlassen verursachte Schäden einzustehen und Ersatz zu leisten.<sup>10</sup> Die vorliegende Arbeit konzentriert sich dabei ausschließlich auf die Haftung derjenigen Organmitglieder der Aktiengesellschaft, die von der Gesellschaft durch einen schuldrechtlichen Vertrag angestellt sind und denen das Aktiengesetz eine besondere Sorgfaltspflicht auferlegt. In der folgenden Betrachtung bezieht sich der Begriff der Organhaftung daher auf das Vorstands- und Aufsichtsratsorgan bzw. deren Organmitglieder. Da der zunehmende Einzug von Anglizismen auch vor dem juristischen Schrifttum nicht Halt macht, werden die Organmitglieder auch als Manager und die Organhaftung analog als Managerhaftung bezeichnet.<sup>11</sup>

Entstandene Schäden sind in Bezug auf die Gesellschaft vor allem in finanziellen Verlusten zu sehen, wohingegen es bei Dritten zu Schäden durch Forderungsausfall insbesondere im Insolvenzfall kommen kann. Ferner können Dritte in ihren absolut geschützten Rechtsgütern<sup>12</sup> geschädigt werden. Das betroffene Organmitglied hat diese Schäden nach §§ 249ff. BGB durch Naturalrestitution oder Geldzahlung zu kompensieren, falls es hierfür haftbar ist.<sup>13</sup>

Von der oben beschriebenen zivilrechtlichen Haftung ist die strafrechtliche Verantwortung zu trennen, die dazu führen kann, dass der Manager zu Geld- und Freiheitsstrafe verurteilt wird. Die Strafgerichtsbarkeit stellt strenge Anforderungen vor allem in Bezug auf die Erhaltung der Vermögenswerte des Unternehmens. Grundlage für eine strafrechtliche Verfolgung von Organmitgliedern sind daher überwiegend die Tatbestände der Untreue oder Unterschlagung.<sup>14</sup> Aber auch im

---

<sup>10</sup> Definition angelehnt an *Thümmel*, Haftung von Managern, 2003, Rn. 18.

<sup>11</sup> Es erscheint aus Sicht der Autoren gerade bei der vorliegenden Thematik sinnvoll, auch die angelsächsisch geprägten Begriffe zu verwenden, da ein Großteil des Schrifttums zum Thema Risikomanagement in englischer Sprache verfasst ist. Weiterhin orientiert sich die Corporate Governance-Diskussion vielfach am angelsächsischen Recht, was im Gegensatz zum deutschen Gesellschaftsrecht eine Zweiteilung des Managements in Vorstand und Aufsichtsrat nicht kennt.

<sup>12</sup> § 823 Abs. 1 BGB fasst hierunter Leben, körperliche Unversehrtheit, Gesundheit, Freiheit, Eigentum und sonstige Rechte.

<sup>13</sup> Siehe *Thümmel*, Haftung von Managern, 2003, Rn. 18.

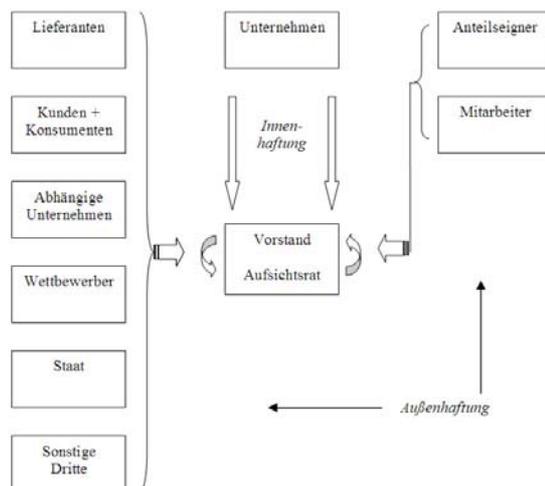
<sup>14</sup> Siehe *Plück/Lattwein*, Haftungsrisiken für Manager, 2004, S. 166.

Bereich der Produkthaftung und des Umweltschutzes sind zunehmend Fälle bekannt.<sup>15</sup>

Das Recht der Managerhaftung ist kein in sich geschlossenes systematisches Regelwerk. Vielmehr bietet es gesetzliche Regelungen jeweils nur für Teilbereiche<sup>16</sup>, was die Komplexität erhöht und die Erfassbarkeit und Überschaubarkeit einschränkt. Für alle in Betracht kommenden Haftungsfälle differenziert das Schrifttum strikt zwischen der so genannten Innenhaftung und Außenhaftung. Dieser auch als „Zweispurigkeit der Haftung“<sup>17</sup> bezeichneten Differenzierung zwischen internen und externen Ansprüchen ist auch in der vorliegenden Arbeit zu folgen, da in der Innen- und Außenhaftung unterschiedliche Anspruchsgrundlagen gelten.

Die Innenhaftung beschreibt die Einstandspflicht des Managers für Schäden, die dem Unternehmen, bei dem er beschäftigt ist, durch sein Fehlverhalten entstanden sind.<sup>18</sup> Während der Bereich der Innenhaftung für die Aktiengesellschaft weitgehend gesetzlich geregelt ist<sup>19</sup>, ist für die Außenhaftung auf das allgemeine Haftungsrecht zurückzugreifen. Unter der Außenhaftung werden die Ansprüche aller möglichen anderen Stakeholder und sonstiger Dritter erfasst. Hierbei handelt es sich um Schadensersatzforderungen deliktischer Natur, für die auf die Tatbestände im Bürgerlichen Gesetzbuch zur unerlaubten Handlung (§§ 823ff. BGB), gegebenenfalls in Verbindung mit Schutzgesetzen, zurückzugreifen ist. Die folgende Darstellung verdeutlicht das Spannungsfeld zwischen Innen- und Außenhaftung, dem die Organe ausgesetzt ist.

### Darstellung 1: Managerhaftung im Überblick



Quelle: *Thümmel, Haftung von Managern, 2003, S. 30.*

<sup>15</sup> Insbesondere vorsätzlich oder fahrlässig begangene Körperverletzungen, zum Beispiel Fälle wie „Milupa“, „Contergan“, „Lederspray“ und „Holzschutzmittel“. Siehe *Schimmer*, Haftung des Vorstands, in: *Europäische Anwaltsvereinigung e.V. (Hrsg.): Managerhaftung, 2001, S. 23 (27); Hauschka*, NJW 2004, S. 257 (258).

<sup>16</sup> Siehe *Thümmel*, Haftung von Managern, 2003, Rn. 19.

<sup>17</sup> *Plück/Lattwein*, Haftungsrisiken für Manager, 2004, S. 18

<sup>18</sup> Siehe *Thümmel*, AG 2004, S. 83.

<sup>19</sup> Für die Aktiengesellschaft insbesondere durch das Aktiengesetz.