

Compliance für die Praxis

Compliance-Risikomanagement

Früherkennung, Prävention und operative Umsetzung

von
Dr. Andreas Kark

1. Auflage

Compliance-Risikomanagement – Kark

schnell und portofrei erhältlich bei beck-shop.de DIE FACHBUCHHANDLUNG

Thematische Gliederung:

[Unternehmensrecht](#)



Verlag C.H. Beck München 2013

Verlag C.H. Beck im Internet:

www.beck.de

ISBN 978 3 406 65370 4

beck-shop.de

Kark
Compliance-Risikomanagement

beck-shop.de

beck-shop.de

Compliance-Risikomanagement

Früherkennung, Prävention
und operative Umsetzung

von

Dr. Andreas Kark, LL.M. (Miami)

Rechtsanwalt in Horb am Neckar



Verlag C.H. Beck München 2013

beck-shop.de

www.beck.de

ISBN 978 3 406 65370 4

© 2013 Verlag C.H. Beck oHG
Wilhelmstraße 9, 80801 München

Druck: Nomos Verlagsgesellschaft,
In den Lissen 12, 76547 Sinzheim

Satz: Textservice Zink, 74869 Schwarzach

Gedruckt auf säurefreiem, alterungsbeständigem Papier
(hergestellt aus chlorfrei gebleichtem Zellstoff)

beck-shop.de

Für Myriam, Anne, Jessica und Dominique

beck-shop.de

Vorwort

Compliance wurde in deutschen Unternehmen lange Zeit als eine Aufgabenstellung betrachtet, die primär von Juristen zu lösen sei. Erst Strafverfahren amerikanischer und deutscher Ermittlungsbehörden gegen große deutsche Unternehmen verdeutlichten auf weithin publizierte Weise, dass Compliance auch ein sehr persönliches Thema werden kann, wenn ein Vorstand oder die Geschäftsführung einer GmbH es versäumt haben, Maßnahmen zu ergreifen, die einem Rechtsbruch aus dem eigenen Unternehmen vorbeugen sollten.

Auch wenn sich mittlerweile die Erkenntnis durchsetzt, dass Compliance zunehmend an Bedeutung gewinnen wird, so besteht noch immer eine nicht geringe Unsicherheit in den Unternehmen, wie man sich diesem doch recht abstrakten Thema nähern soll. Wo setze ich am besten an, wenn ich mein Unternehmen „compliant“ machen möchte?

Voraussetzung jeglicher präventiver Compliance-Maßnahmen ist die Kenntnis der bestehenden Compliance-Risiken. Erst wenn man diese identifiziert hat, kann man wirksame und möglichst ressourcenschonende Präventivmaßnahmen einleiten. Dieses Buch beschreibt die Vorgehensweise bei diesem kritischen ersten Schritt. Anhand von fiktiven Beispielen und durch die Einbindung verschiedener Abbildungen wird anschaulich dargestellt, wie der Prozess des Compliance-Risikomanagements abläuft. Darüber hinaus werden immer wieder Bezüge zu amerikanischen Vorschriften hergestellt, da diese für international tätige Unternehmen ebenfalls immer wichtiger werden.

Dieses praxisorientierte Buch wendet sich an die Mitglieder der Geschäftsleitung von Unternehmen und an die mit Compliance-Themen betrauten Mitarbeiter, die die Compliance-Risiken ihres Unternehmens erfassen und vorhandene Präventivmaßnahmen systematisieren und weiterentwickeln wollen. Darüber hinaus richtet sich dieses Werk auch an Juristen, die ihre Kenntnisse der betriebswirtschaftlichen Aspekte von Compliance erweitern möchten.

Eingang in dieses Buch haben die praktischen Erfahrungen des Autors als Berater von Unternehmen in Compliance-Fragen gefunden sowie seine langjährige Befassung als Mitglied der Geschäftsführung von mehreren ausländischen Tochtergesellschaften eines deutschen Konzerns, für die er für die Umsetzung von Compliance-Anforderungen verantwortlich zeichnete.

Horb am Neckar, April 2013

Andreas Kark

beck-shop.de

Inhaltsverzeichnis

Vorwort	VII
Abbildungsverzeichnis	XIII
Abkürzungsverzeichnis	XV
Literaturverzeichnis	XVII
§ 1. Ausgangssituation	1
§ 2. Rechtliche Bedeutung der Risikofrüherkennung im Unternehmen	5
A. Risikofrüherkennung als Leitungsfunktion	5
I. Der Risikobegriff	6
1. Klassische Unternehmensrisiken	6
a) Finanzwirtschaftliche Unternehmensrisiken	7
aa) Marktrisiken	7
bb) Kreditrisiko	8
cc) Liquiditätsrisiko	8
dd) Rechtsrisiko	8
ee) Betriebsrisiko	8
b) Leistungswirtschaftliche Risiken	8
aa) Risiken bei Forschung und Entwicklung	8
bb) Risiken im Einkauf	9
cc) Risiken in der Produktion	9
dd) Risiken im Vertrieb	9
ee) Risiken in der Logistik	9
c) Bewertung der gängigen Risikoklassifizierungen	9
2. Risikosegmentierung des Deutschen Rechnungslegungs Standards Committee ..	10
3. Compliance-Risiken	12
II. Bestandsgefährdung	16
III. Frühzeitiges Erkennen bestandsgefährdender Risiken	18
IV. Sorgfaltspflicht und Sorgfaltstaat	19
V. Organisations- und Überwachungspflicht	20
VI. Pflichtverletzung	20
VII. Business Judgment Rule	22
1. Unternehmerische Entscheidung	22
2. Handeln zum Wohle der Gesellschaft	24
3. Handeln ohne Sonderinteressen und sachfremde Einflüsse	24
4. Handeln auf der Grundlage angemessener Informationen	24
5. Gutgläubigkeit	26
VIII. Haftung	26
IX. Geltungsbereich	27
1. Geltungsbereich des § 91 Abs. 2 AktG	27
a) Risikoüberwachung in der GmbH	27
b) Risikoüberwachung im Konzern	27
2. Geltungsbereich des § 93 AktG	29
B. Risikofrüherkennung im Deutschen Corporate Governance Kodex	29
I. Inhaltliche Regelung	29
II. Entsprechenserklärung gemäß § 161 AktG	30
C. Fazit	30

§ 3. Das Management von Risiken	31
A. Historischer Überblick	31
I. Risiken verteilen	31
II. Risiken managen	32
III. Fazit	36
B. Risikomanagement im Unternehmen	38
I. Das klassische Risikomanagement	38
1. Bilanzierungs- und steuerrechtliche Vorgaben	39
2. Vorgaben durch Basel II, Basel III und Solvency II	40
a) Basel II	41
b) Basel III	41
c) Basel III und Solvency II	42
d) Unternehmensrating und Compliance-Risiken	42
3. Betriebswirtschaftliche Zielsetzung des Risikomanagements	43
4. Beispiele spezialisierter Risikomanagement-Funktionen	43
a) Treasury-Risikomanagement	44
b) Projekt-Risikomanagement	45
c) Supply-Chain-Risikomanagement	45
d) Umweltrisikomanagement	46
II. Abgrenzung zum Krisenmanagement	47
III. Abgrenzung zum Compliance-Risikomanagement	48
IV. Risikowahrnehmung, Unternehmens- und Risikokultur	49
1. Menschliche Verhaltensmuster bei der Befassung mit Risiken	49
2. Leistungsorientierte Vergütungssysteme	50
3. Heuristische Entscheidungsmethode	51
4. Risikokultur	51
5. Risiken der Risikoberichterstattung	51
a) Fachsprache	52
b) Gestörte Arbeitsbeziehungen	52
c) Risikoexpertise des Managements	52
d) Risikowahrnehmung und Compliance	53
V. Schlussfolgerungen für ein Compliance-Risikomanagement	53
§ 4. Das Management klassischer Unternehmensrisiken	55
A. Prozessschritte des klassischen Risikomanagements	55
I. Definition der Unternehmensrisiken	56
II. Identifizierung der Unternehmensrisiken	57
1. Operative Prozessschritte bei der Identifikation der Unternehmensrisiken	58
a) Abfrage der Unternehmensrisiken in einer Matrixorganisation	58
b) Abfrage der Unternehmensrisiken in einer funktionalen bzw. divisionalen Unternehmensorganisation	62
2. Informationsquellen bei der Risikoidentifikation	63
III. Analyse und Bewertung der Unternehmensrisiken	66
IV. Berichterstattung über Unternehmensrisiken	68
1. Interne Risikoberichterstattung	68
a) Der Vorstand	70
b) Der Aufsichtsrat	70
c) Weitere Adressaten	71
2. Externe Berichterstattung	71
a) Konzernlagebericht gemäß Deutschen Rechnungslegungs Standard Nr. 20	72
aa) Der Prognosebericht	74
bb) Der Risikobericht	74
cc) Der Chancenbericht	78
dd) Internes Kontrollsysteem und Risikomanagementsystem im Konzernrechnungslegungsprozess	78

ee) Weitere Konzernlageberichtsinhalte	79
b) Zwischenberichterstattung gemäß Deutschen Rechnungslegungs Standard Nr. 16	79
aa) Prognose-, Chancen- und Risikobericht	81
bb) Quartalsfinanzberichterstattung	82
cc) Zwischenmitteilungen der Geschäftsführung	83
c) Managementberichterstattung nach IFRS	83
V. Steuerung der Unternehmensrisiken	85
1. Risikostrategie	85
2. Risikokapazität	86
3. Risikotoleranz	86
4. Ertragschancen	87
5. Risikogrenzen	87
6. Maßnahmen der Risikosteuerung	88
a) Risikovermeidung	88
b) Risikoverminderung	89
c) Risikobegrenzung	89
d) Risikowertergabe	90
e) Durch das Unternehmen zu tragende Risiken	90
VI. Risikomonitoring	91
B. Integration in bestehende Unternehmensprozesse	91
I. Die Operative Planung	93
1. Operative Planung der CRM AG 2014–2016	96
2. Organisatorische Einbindung	101
II. Das Risikomanagement in der Operativen Planung	102
C. Organisatorische Einbettung des Risikomanagements	102
D. Fazit	103
§ 5. Das Management von Compliance-Risiken	105
A. Der Prozess des Compliance-Risikomanagements	105
B. Einbettung in bestehende operative Planungsprozesse	106
C. Idealtypischer Compliance-Risikomanagementprozess	106
I. Definition der Compliance-Risiken	107
II. Identifikation der Compliance-Risiken	109
1. Informationsquellen zur Identifizierung von Compliance-Risiken	112
a) Mitarbeiter des Unternehmens	113
b) Führungskräfte und Mitglieder der Geschäftsführung	113
c) Interne Revision	114
d) Rechtsabteilung/Unternehmensanwälte	114
e) Wirtschaftsprüfer	115
f) Internes Kontrollsyste (IKS), Umsetzung des Sarbanes-Oxley Act	115
g) Whistle-Blower	116
h) Wettbewerbsanalyse	117
i) Fazit	118
2. Informationsrücklauf und Dokumentation der Compliance-Risiken	119
III. Analyse und Bewertung der Compliance-Risiken	121
1. Analyse der Compliance-Risiken	121
2. Bewertung identifizierter Compliance-Risiken	121
a) Bemessung der erwarteten Schadenshöhe	122
b) Eintrittswahrscheinlichkeit	124
c) Reputationsschaden	127
IV. Berichterstattung über die Unternehmensrisiken	132
V. Steuerung der Compliance-Risiken	133
1. Compliance-Strategie	133

2. Compliance-Risikokapazität, Compliance-Risikotoleranz, Ertragschancen, Compliance-Risikogrenzen	134
3. Maßnahmen der Compliance-Riskosteuerung	135
a) Compliance-Risikovermeidung	135
b) Compliance-Risikoverminderung	137
c) Compliance-Risikobegrenzung	137
d) Compliance-Risikowertergabe	138
e) Durch das Unternehmen zu tragende Compliance-Risiken	138
VI. Compliance-Riskomonitoring	139
VII. Organisatorische Einbettung	140
VIII. Integration in die Operative Planung	141
D. Compliance-Risikomanagement als integraler Bestandteil der Operativen Planung	141
I. Die Planungsaufforderung zu Compliance-Risiken – Top down Ansatz	142
II. Die Operationalisierung der zentralen Compliance-Vorgaben	143
III. Die dezentrale Bewertung der zentralen Compliance-Vorgaben – bottom up Ansatz	145
1. Das Gegenstromverfahren im Compliance-Risikomanagement	145
2. Der Informationsrücklauf	147
IV. Compliance in der Planungssitzung des Vorstandes	149
V. Compliance in der Planungssitzung des Aufsichtsrates	149
VI. Abschluss von Compliance-Zielvereinbarungen	150
1. Funktionsweise und Bedeutung von Zielvereinbarungen	150
2. Die Compliance-Ziele des Vorstandes	152
3. Compliance-Ziele ins Unternehmen kaskadieren	153
4. Compliance-Zielerreichung	153
E. Fazit und Bewertung des Prozessmodells	153
§ 6. Compliance-Risikomanagement in kleinen und mittelständischen Unternehmen	157
A. Ausgangssituation	157
B. Management klassischer Unternehmensrisiken	158
I. Risikoidentifikation	158
II. Risikosteuerung	162
III. Dokumentation	162
C. Compliance-Risikomanagement	162
I. Compliance-Risikoidentifikation	163
II. Compliance-Risikosteuerung und -dokumentation	163
D. Fazit	164
§ 7. Anglo-amerikanische Anforderungen an das Compliance-Risikomanagement	167
A. US-amerikanische Anforderungen	167
I. US Department of Justice	168
II. US Securities and Exchange Commission	171
III. Gemeinsame Initiative des US Department of Justice und der US Securities and Exchange Commission	174
IV. Fazit	176
B. Der britische Bribery Act 2010	177
I. Guidance zum Bribery Act 2010	178
1. Risk Assessment	178
2. Due Diligence	180
II. Fazit	181
Nachwort	183
Stichwortverzeichnis	185