

Compliance-Risikomanagement

Gefährdungslagen erkennen und steuern

Bearbeitet von
Von Prof. Dr. Andreas Kark, LL.M. (Miami), Rechtsanwalt

2. Auflage 2019. Buch. XXXIV, 280 S. Kartoniert
ISBN 978 3 406 72137 3
Format (B x L): 16,0 x 24,0 cm

[Recht > Handelsrecht, Wirtschaftsrecht > Unternehmensrecht > Compliance](#)

Zu [Leseprobe](#) und [Sachverzeichnis](#)

schnell und portofrei erhältlich bei


DIE FACHBUCHHANDLUNG

Die Online-Fachbuchhandlung beck-shop.de ist spezialisiert auf Fachbücher, insbesondere Recht, Steuern und Wirtschaft. Im Sortiment finden Sie alle Medien (Bücher, Zeitschriften, CDs, eBooks, etc.) aller Verlage. Ergänzt wird das Programm durch Services wie Neuerscheinungsdienst oder Zusammenstellungen von Büchern zu Sonderpreisen. Der Shop führt mehr als 8 Millionen Produkte.

Kark
Compliance-Risikomanagement


beck-shop.de
DIE FACHBUCHHANDLUNG

beck-shop.de
DIE FACHBUCHHANDLUNG

Compliance- Risikomanagement

Gefährdungslagen
erkennen und steuern

von

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

Rechtsanwalt in Horb am Neckar

2., vollständig neu bearbeitete und erweiterte Auflage, 2019

beck-shop.de
DIE FACHBUCHHANDLUNG





beck-shop.de
DIE FACHBUCHHANDLUNG

www.beck.de

ISBN 978 3 406 72137 3

© 2019 Verlag C.H. Beck oHG
Wilhelmstraße 9, 80801 München
Druck: Druckhaus Nomos
In den Lissen 12, 76547 Sinzheim

Satz: 3w+p GmbH, Rimpf
Umschlaggestaltung: Martina Busch, Grafikdesign, Homburg Saar

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

Für Myriam, Anne, Jessica und Dominique

beck-shop.de
DIE FACHBUCHHANDLUNG

beck-shop.de
DIE FACHBUCHHANDLUNG

Vorwort zur 2. Auflage

In den vergangenen Jahren setzte der Begriff „Compliance“ seinen Weg in die Unternehmen in Deutschland weiter fort. Waren es zunächst große börsennotierte Unternehmen, die durch die Justizbehörden vor allem der USA und Deutschlands, aber auch die anderer Länder, gezwungen waren, sicherzustellen, dass Korruptionstaten aufgeklärt werden und durch ein Management der Compliance-Risiken präventiv erneuten Rechtsverstößen aus dem Unternehmen heraus vorgebeugt wird, so ist diese Entwicklung inzwischen sehr viel breiter und auch tiefer in der deutschen Unternehmenswelt verankert.

Diese Entwicklung wird durch große Konzerne unterstützt, die von ihren Zulieferern und Dienstleistern verlangen, dass auch diese ihren Compliance-Anforderungen gerecht werden müssen, wenn sie nicht das Ende der Geschäftsbeziehung riskieren wollen.

Umso erstaunlicher ist es, dass immer wieder zum Teil sehr erhebliche Compliance-Verstöße bekannt werden, und dies selbst in Unternehmen, die umfangreiche Compliance-Managementsysteme etabliert haben. Dabei erreichen manche dieser Gesetzesverstöße Dimensionen, dass in der Presse und seitens der Politik die Frage aufgeworfen wird, inwieweit der Wirtschaftsstandort Deutschland darunter leiden und das Qualitätssiegel „Made in Germany“ in Mitleidenschaft gezogen wird.

Unterstellt man, dass heute einer Unternehmensleitung, ihren Führungskräften und Mitarbeitern im Rahmen von Compliance-Schulungen nahegebracht worden ist, wie wichtig ein rechtlich einwandfreies Verhalten seiner Beschäftigten für den nachhaltigen Erfolg des Unternehmens ist und kann man die entsprechenden rechtlichen Vorgaben als bekannt unterstellen, so können nur andere Mechanismen diese Phänomene erklären.

So wird zum einen anhand dieser Compliance-Verstöße deutlich, dass ein Management von Compliance-Risiken nur dann nachhaltig erfolgreich sein kann, wenn nicht nur die inhaltlichen Vorgaben des Gesetzgebers sowie die der internen Unternehmensrichtlinien bekannt sind. Soll das Compliance-Risikomanagement, und damit das gesamte Compliance-Managementsystem, dauerhaft Gesetzesverstöße unterbinden, muss zum anderen der Vorstand oder die Geschäftsführung eines Unternehmens bereits auf eine entsprechende Gestaltung der Unternehmens- und Compliance-Kultur hinwirken, die ethisch richtiges und damit rechtlich einwandfreies Handeln aller für das Unternehmen Tätigen fördert und fordert.

Daher wurde, neben zahlreichen anderen Ergänzungen, diesem Buch ein weiteres Kapitel zur Bedeutung der Unternehmens- und Compliance-Kultur für ein nachhaltig wirksames Compliance-Risikomanagement hinzugefügt, das auch entsprechende Hinweise enthält, welche Schritte bei einer aktiven Gestaltung der Compliance-Kultur zu beachten sind.

Des Weiteren wurde das Kapitel über die Art und Weise wie wir Menschen mit Risiken umgehen, deutlich erweitert. Ähnlich wie in Bezug auf die aktive Gestaltung einer ethischen Compliance-Kultur ist für Entscheidungsträger, die die Verantwortung für den Erfolg eines präventiven Compliance-Risikomanagements tragen, wichtig zu verstehen, dass es kognitive Defizite des einzelnen Mitarbeiters, der Führungskraft oder des Mitglieds eines Vorstands sind, die zu Compliance-Verstößen führen können. Da wir Menschen uns nicht durch einen als optimal zu beschreibenden Umgang mit Risiken auszeichnen, ist es daher umso wichtiger, diese Defizite durch die Gestaltung einer entsprechenden Prozesslandschaft aufzufangen.

Darüber hinaus kommt dem Aufsichtsrat eine immer wichtigere Rolle zu, auch hinsichtlich seiner Aufgabe, das Management des Compliance-Systems zu überwachen. In einem zusätzlichen Abschnitt wird daher in dieser Auflage erläutert, wie die Mitglieder des Aufsichtsrates die Rechtmäßigkeit, Ordnungsmäßigkeit, Zweckmäßigkeit und Wirtschaftlichkeit des Compliance-Risikomanagementsystems überwachen können.

Die Internationale Organisation für Normung (ISO), wie auch das Institut der Wirtschaftsprüfer (IDW) haben Leitlinien bzw. Standards veröffentlicht, die sich auch mit dem

Management von Compliance-Risiken befassen. Deren inhaltliche Ausgestaltung war ebenfalls im Rahmen eines zusätzlichen Kapitels in dieser Auflage zu beschreiben.

Das Management der Compliance-Risiken eines Unternehmens ermöglicht die begrenzten Ressourcen für die Entwicklung und die Umsetzung effizienter und effektiver Präventivmaßnahmen richtig zu allokkieren, sodass Risiken nicht in Compliance-Verstöße umschlagen. Ein Compliance-Risikomanagement, das auch die „soft facts“ in seinen Prozessen berücksichtigt, stellt sicher, dass das Unternehmen rechtlich einwandfrei und damit nachhaltig tätig ist.

Horb am Neckar, im Dezember 2018

Andreas Kark



beck-shop.de
DIE FACHBUCHHANDLUNG

Vorwort 1. Auflage

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 abstraktem 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, im April 2013

Andreas Kark

beck-shop.de
DIE FACHBUCHHANDLUNG

Inhaltsverzeichnis

Vorwort zur 2. Auflage	VII
Vorwort 1. Auflage	IX
Abbildungsverzeichnis	XVII
Checklistenverzeichnis	XIX
Abkürzungsverzeichnis	XXI
Literaturverzeichnis	XXV

§ 1. Ausgangssituation

§ 2. Rechtliche Bedeutung der Risikofrüherkennung im Unternehmen

A. Risikofrüherkennung als Leitungsfunktion	5
I. Der Risikobegriff	6
1. Klassische Unternehmensrisiken	6
a) Finanzwirtschaftliche Unternehmensrisiken	7
b) Leistungswirtschaftliche Risiken	8
c) Bewertung der gängigen Risikoklassifizierungen	9
2. Risikosegmentierung des Deutsche Rechnungslegungs Standards Committee e.V.	10
3. Compliance-Risiken	12
II. Bestandsgefährdung	16
III. Frühzeitiges Erkennen bestandsgefährdender Risiken	18
IV. Sorgfaltspflicht und Sorgfaltsmaßstab	19
V. Organisations- und Überwachungspflicht	20
VI. Pflichtverletzung	23
VII. Business Judgement Rule	24
1. Unternehmerische Entscheidung	25
2. Handeln zum Wohle der Gesellschaft	26
3. Handeln ohne Sonderinteressen und sachfremde Einflüsse	26
4. Handeln auf der Grundlage angemessener Informationen	27
5. Gutgläubigkeit	28
VIII. Haftung	29
IX. Geltungsbereich	29
1. Geltungsbereich des § 91 Abs. 2 AktG	29
a) Risikoüberwachung in der GmbH	29
b) Risikoüberwachung im Konzern	29
2. Geltungsbereich des § 93 AktG	31
B. Die Überwachung der Risikofrüherkennung durch den Aufsichtsrat	31
I. Allgemeine Vorgaben für die Überwachungstätigkeit des Aufsichtsrates	31
II. Überwachung des Compliance-Risikomanagements	32
C. Risikofrüherkennung im Deutschen Corporate Governance Kodex	34
I. Inhaltliche Regelung	34
II. Entsprechenserklärung gemäß § 161 AktG	34
D. Fazit	35

§ 3. Das Management von Risiken

A. Historischer Überblick	37
I. Risiken verteilen	37
II. Risiken managen	37
III. Fazit	44
B. Risikomanagement im Unternehmen	45
I. Das klassische Risikomanagement	45
1. Bilanzierungs- und steuerrechtliche Vorgaben	45
2. Vorgaben durch Basel II, Basel III und Solvency II	47
a) Basel II	47
b) Basel III	48
c) Basel III und Solvency II	48
d) Unternehmensrating und Compliance-Risiken	49
3. Betriebswirtschaftliche Zielsetzung des Risikomanagements	50
4. Beispiele spezialisierter Risikomanagement-Funktionen	50
a) Treasury-Risikomanagement	51
b) Projekt-Risikomanagement	52
c) Supply-Chain-Risikomanagement	52
d) Umweltrisikomanagement	53
II. Abgrenzung zum Krisenmanagement	54
III. Abgrenzung zum Compliance-Risikomanagement	55
IV. Risikowahrnehmung und Risikokultur	55
1. Schnelles Denken, langsames Denken	56
2. Die menschliche Risikowahrnehmung	56
a) Die sensorische Wahrnehmung	57
b) Der Prozess der Wahrnehmung	58
3. Menschliche Verhaltensmuster bei der Befassung mit Risiken	58
a) Die Prospect Theory	59
b) Heuristische Entscheidungsmethode	60
c) Bestätigungsfehler (confirmation bias)	61
d) Dominanz der ersten Informationen (primacy effect)	61
e) Selbstüberschätzung (overconfidence bias)	61
f) Zwischenergebnis	62
4. Leistungsorientierte Vergütungssysteme	62
5. Risikokultur	64
6. Risiken der Risikoberichterstattung	66
a) Fachsprache	66
b) Gestörte Arbeitsbeziehungen	66
c) Risikoexpertise des Managements	67
d) Risikowahrnehmung und Compliance	67
V. Schlussfolgerungen für ein Compliance-Risikomanagement	68

§ 4. Das Management klassischer Unternehmensrisiken

A. Prozessschritte des klassischen Risikomanagements	71
I. Definition der Unternehmensrisiken	73
II. Identifizierung der Unternehmensrisiken	74
1. Operative Prozessschritte bei der Identifikation der Unternehmensrisiken	74
a) Abfrage der Unternehmensrisiken in einer Matrixorganisation	75
b) Abfrage der Unternehmensrisiken in einer funktionalen bzw. divisionalen Unternehmensorganisation	78
2. Informationsquellen bei der Risikoidentifikation	80

III. Analyse und Bewertung der Unternehmensrisiken	82
IV. Berichterstattung über Unternehmensrisiken	84
1. Interne Risikoberichterstattung	85
a) Der Vorstand	86
b) Der Aufsichtsrat	86
c) Weitere Adressaten	87
2. Externe Berichterstattung	88
a) Konzernlagebericht gemäß Deutschen Rechnungslegungs Standard Nr. 20	88
b) Halbjahresfinanzberichterstattung gemäß Deutschen Rechnungslegungs Standard Nr. 16	97
c) Managementberichterstattung nach IFRS	100
V. Steuerung der Unternehmensrisiken	102
1. Risikostrategie	102
2. Risikokapazität	103
3. Risikotoleranz	103
4. Ertragschancen	104
5. Risikogrenzen	104
6. Maßnahmen der Risikosteuerung	105
a) Risikovermeidung	105
b) Risikoverminderung	106
c) Risikobegrenzung	106
d) Risikoweitergabe	107
e) Durch das Unternehmen zu tragende Risiken	107
VI. Risikomonitoring	108
B. Integration in bestehende Unternehmensprozesse	109
I. Die Operative Planung	110
1. Operative Planung der CRM AG 2020–2022	113
2. Organisatorische Einbindung	118
II. Das Risikomanagement in der Operativen Planung	118
C. Organisatorische Einbettung des Risikomanagements	119
D. Fazit	120
§ 5. Das Management von Compliance-Risiken	
A. Der Prozess des Compliance-Risikomanagements	121
B. Einbettung in bestehende operative Planungsprozesse	122
C. Idealtypischer Compliance-Risikomanagementprozess	122
I. Definition der Compliance-Risiken	123
II. Identifikation der Compliance-Risiken	125
1. Informationsquellen zur Identifizierung von Compliance-Risiken	128
a) Mitarbeiter des Unternehmens	128
b) Führungskräfte und Mitglieder der Geschäftsleitung	129
c) Interne Revision	129
d) Rechtsabteilung/Unternehmensanwälte	130
e) Wirtschaftsprüfer	130
f) Internes Kontrollsystem (IKS), Umsetzung des Sarbanes-Oxley Act	131
g) Whistleblower	132
h) Wettbewerbsanalyse	132
i) Fazit	133
2. Informationsrücklauf und Dokumentation der Compliance-Risiken	135

III. Analyse und Bewertung der Compliance-Risiken	137
1. Analyse der Compliance-Risiken	137
2. Bewertung identifizierter Compliance-Risiken	138
a) Bemessung der erwarteten Schadenshöhe	138
b) Eintrittswahrscheinlichkeit	140
c) Reputationsschaden	143
IV. Berichterstattung über die Compliance-Risiken	149
V. Steuerung der Compliance-Risiken	149
1. Compliance-Strategie	150
2. Compliance-Risikokapazität, Compliance-Risikotoleranz, Ertragschancen, Compliance-Risikogrenzen	150
3. Maßnahmen der Compliance-Risikosteuerung	151
a) Compliance-Risikovermeidung	152
b) Compliance-Risikoverminderung	153
c) Compliance-Risikobegrenzung	153
d) Compliance-Risikoweitergabe	153
e) Durch das Unternehmen zu tragende Compliance-Risiken	154
VI. Compliance-Risikomonitoring	155
VII. Organisatorische Einbettung	156
VIII. Integration in die Operative Planung	157
D. Compliance-Risikomanagement als integraler Bestandteil der Operativen Planung	158
I. Die Planungsaufforderung zu Compliance-Risiken – Top-Down Ansatz ...	158
II. Die Operationalisierung der zentralen Compliance-Vorgaben	159
III. Die dezentrale Bewertung der zentralen Compliance-Vorgaben – Bottom-Up Ansatz	162
1. Das Gegenstromverfahren im Compliance-Risikomanagement	162
2. Der Informationsrücklauf	164
IV. Compliance in der Planungssitzung des Vorstandes	165
V. Compliance in der Planungssitzung des Aufsichtsrates	166
VI. Abschluss von Compliance-Zielvereinbarungen	166
1. Funktionsweise und Bedeutung von Zielvereinbarungen	167
2. Die Compliance-Ziele des Vorstandes	169
3. Compliance-Ziele ins Unternehmen kaskadieren	170
4. Compliance-Zielerreichung	170
E. Fazit und Bewertung des Prozessmodells	171
§ 6. Compliance-Risikomanagement in kleinen und mittelständischen Unternehmen	
A. Ausgangssituation	173
B. Management klassischer Unternehmensrisiken	174
I. Risikoidentifikation	174
II. Risikosteuerung	177
III. Dokumentation	177
C. Compliance-Risikomanagement	178
I. Compliance-Risikoidentifikation	178
II. Compliance-Risikosteuerung und -dokumentation	180
D. Fazit	181

§ 7. Compliance-Risikomanagementstandards der ISO und des IDW

A. Die Standards der ISO	185
I. Das Compliance-Risikomanagement in den Compliance-Managementsysteme-Leitlinien DIN ISO 19600	186
II. Das Compliance-Risikomanagement in den Leitlinien und Anmerkungen zu „Managementsysteme zur Korruptionsbekämpfung“ (ISO 37001:2016)	189
III. Das Compliance-Risikomanagement im Entwurf der Leitlinien zum Risikomanagement ISO 31000	193
IV. Kritische Würdigung	194
1. Die Leitlinien als Weg zur Integration von Compliance in die Geschäftsprozesse	194
2. Die Leitlinien aus der Perspektive des Compliance-Risikomanagements	195
B. Die Prüfungsstandards des IDW	197
I. Das Compliance-Risikomanagement in den Grundsätzen ordnungsmäßiger Prüfung von Compliance Management Systemen (IDW PS 980)	197
II. Das Compliance-Risikomanagement in den Grundsätzen ordnungsmäßiger Prüfung von Risikomanagementsystemen (IDW PS 981)	200
III. Kritische Würdigung	201

**§ 8. Anglo-amerikanische Anforderungen an das
Compliance-Risikomanagement**

A. US-amerikanische Anforderungen	203
I. US Department of Justice	204
II. US Securities and Exchange Commission	207
III. Gemeinsame Initiative des US Department of Justice und der US Securities and Exchange Commission	209
IV. Fazit	211
B. Der britische Bribery Act 2010	213
I. Guidance zum Bribery Act 2010	213
1. Risk Assessment	214
2. Due Diligence	216
II. Fazit	216

**§ 9. Compliance-Kultur als Grundvoraussetzung eines erfolgreichen
Compliance-Risikomanagements**

A. Unternehmenskultur, wertorientierte Führung und Unternehmenserfolg	218
I. Unternehmenskultur als Begriff	219
1. Die betriebswirtschaftliche Perspektive	219
2. Die sozial- und organisationspsychologische Perspektive	219
a) Artefakte	220
b) Gewählte Überzeugungen und Werte	221
c) Selbstverständliche, grundlegende Annahmen	223
II. Die Bedeutung der Unternehmenskultur für Mitarbeiter und das Unternehmen	224
1. Die Bedeutung der Unternehmenskultur für den Mitarbeiter	224
2. Die Bedeutung der Unternehmenskultur für das Unternehmen und dessen Compliance	225

B. Die Compliance-Kultur	227
I. Compliance-Kultur als Begriff	228
1. Compliance-Kultur aus der Sicht des US Department of Justice und der US Securities and Exchange Commission	228
2. Compliance-Kultur aus deutscher Sicht	229
3. Interdisziplinäres Verständnis einer nachhaltigen Compliance-Kultur	230
a) Das Billigkeitsverständnis bei Aristoteles	231
b) Compliance als selbstverständliche, grundlegende Annahme	231
II. Compliance-Risiken und Compliance-Kultur	232
1. Drei Perspektiven auf Compliance-Risiken	232
a) Vom ehrbaren Kaufmann zur Corporate Social Responsibility	232
b) Von der Gewinnmaximierung zu nützlichen Rechtsverletzungen	233
c) Vom ehrbaren Kaufmann bis zum Homo oeconomicus	234
2. Der Eigennutz als Compliance-Risiko	234
3. Die Mehrdeutigkeit, Vielfalt und Durchsetzung gesetzlicher Vorschriften als Compliance-Risiko	235
4. Die moralischen Entwicklungsstufen des Menschen als Compliance-Risiko	235
III. Möglichkeiten zur Gestaltung der Compliance-Kultur	238
1. Die ethische Infrastruktur des Unternehmens	239
a) Formelle Systeme	240
b) Informelle Systeme	242
2. Die interpersonellen Beziehungen	245
a) Der sozial-kognitive Lernprozess	245
b) Die moralische Entkoppelung	246
c) Der Einfluss der Kollegen	247
d) Der Einfluss der Vorgesetzten	248
e) Der Einfluss des Vorstandes	249
3. Schlussfolgerungen für die operative Gestaltung der Compliance-Kultur	249
a) Artefakte schaffen	251
b) Vorbild geben und ein fürsorgliches Klima schaffen	252
c) Personalpolitik	253
C. Fazit	254
Nachwort zur 2. Auflage	257
Nachwort	259
Zusammenfassung der Checklisten	261
Stichwortverzeichnis	275