

# Inhaltsverzeichnis

Vorwort zur 3. Auflage .....	VII
Vorwort zur 2. Auflage .....	IX
Vorwort 1. Auflage .....	XI
Abkürzungsverzeichnis .....	XXI
Verzeichnis der (abgekürzt) zitierten Literatur .....	XXV
Gesetzessammlungen und ergänzende Materialien .....	XXXV
Abbildungsverzeichnis .....	XXXVII
Checklistenverzeichnis .....	XXXIX

## § 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 .....	10
2. Risikosegmentierung des Deutsche Rechnungslegungs Standards Committee e.V. ....	10
3. Compliance-Risiken .....	12
II. Bestandsgefährdung .....	17
III. Frühzeitiges Erkennen bestandsgefährdender Risiken .....	19
IV. Sorgfaltspflicht und Sorgfaltsmaßstab .....	20
V. Organisations- und Überwachungspflicht .....	21
VI. Pflichtverletzung .....	23
VII. Business Judgement Rule .....	25
1. Unternehmerische Entscheidung .....	25
2. Handeln zum Wohle der Gesellschaft .....	26
3. Handeln ohne Sonderinteressen und sachfremde Einflüsse .....	27
4. Handeln auf der Grundlage angemessener Informationen .....	27
5. Gutgläubigkeit .....	29
VIII. Haftung .....	29
IX. Geltungsbereich .....	29
1. Geltungsbereich des § 91 Abs. 2 AktG .....	29
a) Risikoüberwachung in der GmbH .....	30
b) Risikoüberwachung im Konzern .....	30
2. Geltungsbereich des § 93 AktG .....	32
B. Die Überwachung der Risikofrüherkennung durch den Aufsichtsrat .....	32
I. Allgemeine Vorgaben für die Überwachungstätigkeit des Aufsichtsrates .....	32
II. Überwachung des Compliance-Risikomanagements .....	33
C. Risikofrüherkennung im Deutschen Corporate Governance Kodex .....	35
I. Inhaltliche Regelung .....	35
II. Entsprechenserklärung gemäß § 161 AktG .....	35
D. Fazit .....	36

### § 3. Das Management von Risiken

A. Historischer Überblick .....	37
I. Risiken verteilen .....	37
II. Risiken managen .....	37
III. Fazit .....	44
B. Risikomanagementim Unternehmen .....	44
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 .....	51
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 .....	57
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 .....	65
a) Fachsprache .....	66
b) Gestörte Arbeitsbeziehungen .....	66
c) Risikoexpertise des Managements .....	66
d) Risikowahrnehmung und Compliance .....	67
V. Schlussfolgerungen für ein Compliance-Risikomanagement .....	67

### § 4. Das Management klassischer Unternehmensrisiken

A. Prozessschritte des klassischen Risikomanagements .....	69
I. Definition der Unternehmensrisiken .....	72
II. Identifizierung der Unternehmensrisiken .....	72
1. Operative Prozessschritte bei der Identifikation der Unternehmensrisiken .....	73
a) Abfrage der Unternehmensrisiken in einer Matrixorganisation .....	73
b) Abfrage der Unternehmensrisiken in einer funktionalen bzw. divisionalen Unternehmensorganisation .....	77

2. Informationsquellen bei der Risikoidentifikation .....	79
III. Analyse und Bewertung der Unternehmensrisiken .....	81
IV. Berichterstattung über Unternehmensrisiken .....	83
1. Interne Risikoberichterstattung .....	84
a) Der Vorstand .....	85
b) Der Aufsichtsrat .....	85
c) Weitere Adressaten .....	86
2. Externe Berichterstattung .....	87
a) Konzernlagebericht gemäß Deutschen Rechnungslegungs Standard Nr. 20 .....	87
b) Halbjahresfinanzberichterstattung gemäß Deutschen Rechnungslegungs Standard Nr. 16 .....	96
c) Managementberichterstattung nach IFRS .....	99
V. Steuerung der Unternehmensrisiken .....	100
1. Risikostrategie .....	101
2. Risikokapazität .....	102
3. Risikotoleranz .....	103
4. Ertragschancen .....	103
5. Risikogrenzen .....	103
6. Maßnahmen der Risikosteuerung .....	104
a) Risikovermeidung .....	104
b) Risikoverminderung .....	105
c) Risikobegrenzung .....	105
d) Risikoweitergabe .....	106
e) Durch das Unternehmen zu tragende Risiken .....	106
VI. Risikomonitoring .....	107
B. Integration in bestehende Unternehmensprozesse .....	108
I. Die Operative Planung .....	109
1. Operative Planung der CRM AG 2024–2026 .....	112
2. Organisatorische Einbindung .....	117
II. Das Risikomanagement in der Operativen Planung .....	117
C. Organisatorische Einbettung des Risikomanagements .....	118
D. Fazit .....	119
 <b>§ 5. Das Management von Compliance-Risiken</b>	
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- und Hinweisgebersysteme .....	132
h) Wettbewerbsanalyse .....	137
i) Fazit .....	138

2. Informationsrücklauf und Dokumentation der Compliance-Risiken .....	141
III. Analyse und Bewertung der Compliance-Risiken .....	142
1. Analyse der Compliance-Risiken .....	142
2. Bewertung identifizierter Compliance-Risiken .....	143
a) Bemessung der möglichen Gesamtschadenshöhe .....	144
b) Eintrittswahrscheinlichkeit .....	147
c) Reputationsschaden .....	151
IV. Berichterstattung über die Compliance-Risiken .....	157
V. Steuerung der Compliance-Risiken – das Compliance-Programm .....	157
1. Compliance-Strategie .....	158
2. Compliance-Risikokapazität, Compliance-Risikotoleranz, Ertragschancen, Compliance-Risikogrenzen .....	158
3. Maßnahmen der Compliance-Risikosteuerung .....	159
a) Compliance-Risikovermeidung .....	160
b) Compliance-Risikoverminderung .....	161
c) Compliance-Risikobegrenzung .....	162
d) Compliance-Risikoweitergabe .....	162
e) Durch das Unternehmen zu tragende Compliance-Risiken .....	162
f) Die Brutto- und Nettobewertung der Compliance-Risiken .....	163
VI. Compliance-Risikomonitoring .....	166
VII. Organisatorische Einbettung .....	167
VIII. Integration in die Operative Planung .....	168
D. Compliance-Risikomanagement als integraler Bestandteil der Operativen Planung .....	168
I. Die Planungsaufforderung zu Compliance-Risiken – Top-Down Ansatz .....	169
II. Die Operationalisierung der zentralen Compliance-Vorgaben .....	170
III. Die dezentrale Bewertung der zentralen Compliance-Vorgaben – Bottom-Up Ansatz .....	172
1. Das Gegenstromverfahren im Compliance-Risikomanagement .....	172
2. Der Informationsrücklauf .....	174
IV. Compliance in der Planungssitzung des Vorstandes .....	175
V. Compliance in der Planungssitzung des Aufsichtsrates .....	176
VI. Abschluss von Compliance-Zielvereinbarungen .....	176
1. Funktionsweise und Bedeutung von Zielvereinbarungen .....	177
2. Die Compliance-Ziele des Vorstandes .....	179
3. Compliance-Ziele ins Unternehmen kaskadieren .....	180
4. Compliance-Zielerreichung .....	180
E. Compliance-Risikoaudit .....	180
F. Fazit und Bewertung des Prozessmodells .....	184
 <b>§ 6. Compliance-Risikomanagement in kleinen und mittelständischen Unternehmen</b>	
A. Ausgangssituation .....	187
B. Management klassischer Unternehmensrisiken .....	188
I. Risikoidentifikation .....	188
II. Risikosteuerung .....	191
III. Dokumentation .....	191
C. Compliance-Risikomanagement .....	192
I. Compliance-Risikoidentifikation .....	192
II. Compliance-Risikosteuerung und -dokumentation .....	194

D. Fazit .....	195
----------------	-----

## **§ 7. Compliance-Risikomanagementstandards der ISO und des IDW**

A. Die Standards der ISO .....	199
I. Das Compliance-Risikomanagement in den „Compliance-Managementsysteme – Anforderungen mit Leitlinien zur Anwendung“ (ISO 37301) .....	200
II. Das Compliance-Risikomanagement in den Leitlinien und Anmerkungen zu „Managementsysteme zur Korruptionsbekämpfung“ (ISO 37001:2016) .....	203
III. Das Compliance-Risikomanagement in den Leitlinien zum Risikomanagement ISO 31000 .....	207
IV. Das Compliance-Risikomanagement in Hinweismanagementsysteme – Leitlinien (ISO 37002:2021) .....	208
V. Kritische Würdigung .....	209
1. Die Leitlinien als Weg zur Integration von Compliance in die Geschäftsprozesse .....	209
2. Die Leitlinien aus der Perspektive des Compliance-Risikomanagements .....	210
B. Die Prüfungsstandards des IDW .....	211
I. Das Compliance-Risikomanagement in dem IDW Prüfungsstandard: Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen (IDW PS 980 n.F. (09.2022)) .....	212
II. Das Compliance-Risikomanagement in den Grundsätzen ordnungsmäßiger Prüfung von Risikomanagementsystemen (IDW PS 981) .....	215
III. Kritische Würdigung .....	216
III. Das Compliance-Risikomanagement in der Neufassung des IDW Prüfungsstandards: Die Prüfung des Risikofrüherkennungssystems (IDW PS 340 n.F.) .....	217

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

A. US-amerikanische Anforderungen .....	219
I. US Department of Justice .....	220
II. US Securities and Exchange Commission .....	223
III. Gemeinsame Initiative des US Department of Justice und der US Securities and Exchange Commission .....	225
III. US Department of Justice, Criminal Division – Überprüfung der Wirksamkeit eines Compliance-Managementsystems .....	227
IV. Fazit .....	234
B. Der britische Bribery Act 2010 .....	238
I. Guidance zum Bribery Act 2010 .....	239
1. Risk Assessment .....	239
2. Due Diligence .....	241
II. Fazit .....	241

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

A. Unternehmenskultur, werteorientierte Führung und Unternehmenserfolg .....	244
I. Unternehmenskultur als Begriff .....	245
1. Die betriebswirtschaftliche Perspektive .....	245

2. Die sozial- und organisationspsychologische Perspektive .....	245
a) Artefakte .....	246
b) Gewählte Überzeugungen und Werte .....	247
c) Selbstverständliche, grundlegende Annahmen .....	249
II. Die Bedeutung der Unternehmenskultur für Mitarbeiter und das Unternehmen .....	250
1. Die Bedeutung der Unternehmenskultur für den Mitarbeiter .....	250
2. Die Bedeutung der Unternehmenskultur für das Unternehmen und dessen Compliance .....	251
B. Die Compliance-Kultur .....	254
I. Compliance-Kultur als Begriff .....	254
1. Compliance-Kultur aus der Sicht des US Department of Justice und der US Securities and Exchange Commission .....	254
2. Compliance-Kultur aus deutscher Sicht .....	255
3. Interdisziplinäres Verständnis einer nachhaltigen Compliance-Kultur .....	256
a) Das Billigkeitsverständnis bei Aristoteles .....	257
b) Compliance als selbstverständliche, grundlegende Annahme .....	257
II. Compliance-Risiken und Compliance-Kultur .....	258
1. Drei Perspektiven auf Compliance-Risiken .....	258
a) Vom ehrbaren Kaufmann zur Corporate Social Responsibility .....	258
b) Von der Gewinnmaximierung zu nützlichen Rechtsverletzungen .....	259
c) Vom ehrbaren Kaufmann bis zum Homo oeconomicus .....	260
2. Der Eigennutz als Compliance-Risiko .....	260
3. Die Mehrdeutigkeit, Vielfalt und Durchsetzung gesetzlicher Vorschriften als Compliance-Risiko .....	261
4. Die moralischen Entwicklungsstufen des Menschen als Compliance-Risiko .....	261
5. Fehlende psychologische Sicherheit im Unternehmen als Compliance-Risiko .....	264
III. Möglichkeiten zur Gestaltung der Compliance-Kultur .....	271
1. Die ethische Infrastruktur des Unternehmens .....	273
a) Formelle Systeme .....	273
b) Informelle Systeme .....	275
2. Die interpersonellen Beziehungen .....	278
a) Der sozial-kognitive Lernprozess .....	278
b) Die moralische Entkoppelung .....	279
c) Der Einfluss der Kollegen .....	280
d) Der Einfluss der Vorgesetzten .....	281
e) Der Einfluss des Vorstandes .....	282
3. Schlussfolgerungen für die operative Gestaltung der Compliance-Kultur .....	282
a) Artefakte schaffen .....	284
b) Vorbild geben und ein fürsorgliches Klima schaffen .....	285
c) Personalpolitik .....	286

C. Fazit ..... 287

Nachwort zur 3. Auflage ..... 289

Nachwort zur 2. Auflage ..... 290

Nachwort ..... 292

Zusammenfassung der Checklisten ..... 293

Sachverzeichnis ..... 313