Compliance-Risikoanalyse

Moosmayer

2. Auflage 2020
ISBN 978-3-406-73368-0
C.H.BECK

schnell und portofrei erhältlich bei
beck-shop.de

Die Online-Fachbuchhandlung beck-shop.de steht für Kompetenz aus Tradition. Sie gründet auf über 250 Jahre juristische Fachbuch-Erfahrung durch die Verlage C.H.BECK und Franz Vahlen.
beck-shop.de hält Fachinformationen in allen gängigen Medienformaten bereit: über 12 Millionen Bücher, eBooks, Loseblattwerke, Zeitschriften, DVDs, Online-Datenbanken und Seminare. Besonders geschätzt wird beck-shop.de für sein umfassendes Spezialsortiment im Bereich Recht, Steuern und Wirtschaft mit rund 700.000 lieferbaren Fachbuchtiteln.

Moosmayer
Compliance-Risikoanalyse

beck-shop.de
DIE FACHBUCHHANDLUNG

beck-shop.de
DIE FACHBUCHHANDLUNG

Compliance-Risikoanalyse

Praxisleitfaden für Unternehmen

Herausgegeben von

Dr. Klaus Moosmayer

2. Auflage 2020

beck-shop.de
DIE FACHBUCHHANDLUNG

C.H.BECK

Zitiervorschlag:
Moosmayer Compliance Risikoanalyse/*Bearbeiter* § … Rn. …

beck-shop.de
DIE FACHBUCHHANDLUNG

www.beck.de

ISBN 978 3 406 73368 0

© 2020 Verlag C.H. Beck oHG
Wilhelmstraße 9, 80801 München
Druck: Druckhaus Nomos
In den Lissen 12, 76547 Sinzheim

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

CO_2 neutral
chbeck.de/nachhaltig

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

Vorwort

Schon in meinem Vorwort zur 1. Auflage, erschienen 2015, habe ich darauf hingewiesen, wie wichtig es ist, Compliance und Compliance Management aus der Risikoperspektive zu sehen. Nur sie bietet für Compliance als einer der bedeutendsten Assurance Funktionen im Unternehmen den richtigen Ordnungsrahmen und Referenzpunkt. Ich würde heute noch weiter gehen: Nur ein konsequent aus der Risikoperspektive verstandenes und umgesetztes Compliance Management erzeugt bei Unternehmensangehörigen und Stakeholders die Akzeptanz, die es verdient und braucht, um wirksam zu sein.

Klaus Moosmayer und seine Mitautoren zeichnen nicht nur den rechtlichen Rahmen für die Compliance Risikoanalyse in Deutschland kompakt und eingängig. Sie bieten darüber hinaus vor allem praktische Anleitung für deren Implementierung in Unternehmen. Compliance ist keine akademische Übung und schon gar keine, in der es genügt, sein Recht zu kennen. Compliance geht weit darüber hinaus. Nur wer sich der Zusammenhänge zwischen den compliance-relevanten Schlüsselprozessen in der Interaktion des Unternehmens mit seinen Stakeholders bewusst ist und nur wer die Risiken an den kritischen Stellen dieser Prozesse kennt, wird wirksames Compliance Management betreiben können.

Ob Compliance Management von Stakeholders inner- und außerhalb des Unternehmens als wichtiger Beitrag zur Sicherung des Unternehmens gesehen wird, hängt sodann stark davon ab, dass es gelingt, den Nutzen wirksamer Compliance sichtbar zu machen. Dies wiederum ist unmittelbare Folge davon, dass die Risiken von Non-Compliance bewusst gemacht werden. Sind diese Risiken evident, sind Unternehmensangehörige stärker motiviert, sich regelkonform zu verhalten und sie erleben Compliance als sinnstiftend.

In diesem Sinne bleibt das von Klaus Moosmayer herausgegebene Werk auch in seiner 2. Auflage Pflichtlektüre für alle, die in der Verantwortung stehen, Unternehmen sicher in die Zukunft zu führen. Ich wünsche dem vorliegenden Werk ebenso viel Erfolg wie der 1. Auflage.

beck-shop.de
DIE FACHBUCHHANDLUNG

St. Gallen, im März 2020 *Prof. Dr. Leo Staub*, Rechtsanwalt

beck-shop.de
DIE FACHBUCHHANDLUNG

Bearbeiterverzeichnis

Prof. Dr. Dr. h.c. Werner Beulke
Rechtsanwalt in Passau

Hubertus Eichler
Wirtschaftsprüfer und Steuerberater in München

Dr. Alexander Eufinger
Leiter Personal & Recht der Stiftung Hospital zum Heiligen Geist, Frankfurt a. M.

Dr. Anabel Harting
Rechtsanwältin bei HengelerMueller, Frankfurt a. M.

Dr. Wolfgang Heckenberger
Rechtsanwalt, Senior Competition Advisor der Siemens AG, München

Dipl.-Ing. Volker Klasen
Siemens AG, Leiter Compliance Risk, Framework & Controls, Erlangen

Dr. Philip Matthey, LL.M.
Rechtsanwalt, Chief Compliance Officer bei TRATON SE, München
Vorstandsmitglied von DICO – Deutsches Institut für Compliance e.V., Berlin

Dr. Klaus Moosmayer
Mitglied der Geschäftsleitung Novartis, Chief Ethics,
Risk and Compliance Officer, Basel

Dipl.-Kfm. Meinhard Remberg
Generalbevollmächtigter bei der SMS GmbH, Hilchenbach,
und Vorstandssprecher von DICO – Deutsches Institut für Compliance e.V., Berlin

Dr. Anita Schieffer
Chief Compliance Officer Siemens Energy, Siemens Gas & Power GmbH & Co. KG,
München

Dipl.-Wirtsch.-Ing. Jan Schreiner
Abteilungsleiter GRC – Risks & Projects bei TRATON SE, München

Dr. Robert Schulz
Rechtsanwalt und Head of Legal – Sales & Marketing bei der BSH Hausgeräte GmbH,
München

Dipl.-Verww. (FH) Ingo Sorgatz
Erster Kriminalhauptkommissar, Bundesministerium des Innern, für Bau und Heimat,
Berlin

Dr. Christian Steinle
Partner und Rechtsanwalt bei Gleiss Lutz, Stuttgart

beck-shop.de
DIE FACHBUCHHANDLUNG

Prof. Dr. Jochen Vetter
Partner und Rechtsanwalt bei HengelerMueller, München;
Honorarprofessor an der Universität zu Köln

Dr. Antonie Wauschkuhn
Leiterin Compliance Europa und CIS der Siemens AG, München

Heiko Wendel
Rechtsanwalt, General Counsel & Chief Compliance Officer der
FUCHS PETROLUB SE, Mannheim

Dipl.-Jur. Mathias Wendt
Unternehmensberater, 7C-Consulting GmbH, Berlin

Dr. Tobias Witzigmann
Bayerisches Staatsministerium der Justiz

beck-shop.de
DIE FACHBUCHHANDLUNG

Inhaltsverzeichnis

Vorwort V
Bearbeiterverzeichnis VII
Abkürzungsverzeichnis XV
Verzeichnis der (abgekürzt) zitierten Literatur XIX

Kapitel 1. Einführung

A. Anlass für eine Compliance-Risikoanalyse 1
B. Rechtliche Bedeutung und Quellen der Compliance-Risikoanalyse 2
C. Systematik und Durchführung der Compliance-Risikoanalyse 5

Kapitel 2. Rechtliche Grundlagen der Compliance Risikoanalyse und Umsetzung im Unternehmen

§ 1. Überblick zu den straf- bzw. ordnungswidrigkeitenrechtlich relevanten Organisations- und Aufsichtspflichten im Unternehmen 9
A. Strafrechtlich implizierte Organisations- und Aufsichtspflichten 10
I. Pflicht zur Vermeidung bzw. Kontrolle betriebsbezogener Gefahren 10
1. Sachliche Gefahrenquellen für Leib und Leben Dritter 10
2. Personale „Gefahrenquellen" – Pflicht zum Einschreiten gegen Straftaten Beschäftigter 11
3. Erfordernis der „Betriebsbezogenheit" 13
4. Verantwortungsverteilung innerhalb des Unternehmens 14
5. Inhalt der Garantenpflichten 15
6. Strafbarkeitsvoraussetzungen jenseits der Garantenpflicht 16
II. Sonstige strafrechtlich implizierte Organisations- und Aufsichtspflichten 17
III. Drohende Sanktionen bei Verletzung der Organisations- und Aufsichtspflichten 18
1. Kriminalstrafe 18
2. Einziehung 20
B. Ordnungswidrigkeitenrechtlich implizierte Organisations- und Aufsichtspflichten 22
I. Organisations- und Aufsichtspflichten nach Maßgabe des § 130 OWiG 22
1. Das Unterlassen notwendiger Aufsichtsmaßnahmen als Tathandlung 22
2. Der Täterkreis des § 130 OWiG 25
3. Weitere Voraussetzungen einer Ahndung gem. § 130 Abs. 1 OWiG 26
II. Sonstige ordnungswidrigkeitenrechtlich implizierte Aufsichts- und Organisationspflichten 27
III. Drohende Sanktionen bei Verletzung der Organisations- und Aufsichtspflichten 27
1. Geldbuße gegen natürliche Personen 27
2. Verbandsgeldbuße 27
3. Einziehung 30

§ 2. Überblick der gesellschaftsrechtlichen Organisations- und Aufsichtspflichten im Unternehmen 31
A. Vorbemerkung 31

beck-shop.de
DIE FACHBUCHHANDLUNG

B. Allgemeine Organisations- und Aufsichtspflichten im Einzelunternehmen 32
I. Pflichten des Vorstands 32
1. Pflicht zur Einrichtung eines Risikofrüherkennungssystems (§ 91 Abs. 2 AktG) 32
2. Risikoanalyse als Teil der allgemeinen Leitungsaufgabe (§§ 76, 93 AktG) 37
II. Pflichten des Aufsichtsrats 40
1. Gegenstand der Überwachung im Bereich des Risikomanagements 40
2. Mittel zur Überwachung des Risikomanagements durch den Aufsichtsrat 41
3. Delegation der Überwachung des Risikomanagements an einen Prüfungsausschuss 42
C. Organisations- und Aufsichtspflichten im Konzern 43
I. Pflichten des Vorstands 43
1. Vorstand der herrschenden Gesellschaft 43
2. Vorstand der abhängigen Gesellschaft 45
II. Pflichten des Aufsichtsrats 46
D. Haftungsrisiken bei Verletzung der Organisations- und Aufsichtspflichten 46
I. Haftungsrisiken der Vorstandsmitglieder 46
II. Haftungsrisiken der Aufsichtsratsmitglieder 47

§ 3. Praktische Umsetzung der Compliance-Anforderungen im Unternehmen 48
A. Ausgangspunkt: Haftungsrisiken für Unternehmensverantwortliche im Bereich der Organisations- und Aufsichtspflichten 48
B. Maßnahmen zur Umsetzung der gesetzlichen Anforderungen 50
I. Grundüberlegungen 50
1. Parameter für eine Risikoanalyse 50
2. Umsetzung im Rahmen eines Compliance Management Systems 51
II. Organisations- und Aufsichtspflichten in der Unternehmenspraxis 52
1. Sorgfältige Auswahl von Mitarbeitern 52
2. Organisatorische Anforderungen 53
3. Aufklärung und Unterweisung der Mitarbeiter 57
4. Unterweisung der Führungskräfte 59
5. Überwachung und Kontrolle 60
III. Aufdeckung und Sanktionierung von Verstößen 65
1. Aufklärung und Untersuchung 65
2. Offenlegung von Verstößen an die Behörden? 66
3. Sanktionierung und Beseitigung der Missstände 67
C. Umsetzung der gesetzlichen Verpflichtungen im Konzern 67
I. Berichtspflichten und Auskunftsrechte der Konzernmutter 69
II. Organisation und Instrumente der Konzernsteuerung 69
1. Konzernweite Berichtslinien 69
2. Konzernweite Steuerung 69
D. Zusammenfassung und Ausblick 70

Kapitel 3. Praxisbeispiele der Compliance-Risikoanalyse aus Verwaltung und Unternehmen

§ 4. Compliance-Risikoanalyse im Unternehmen am Beispiel von TRATON 73
A. Hintergrund 73
I. Historie, Geschäftstätigkeit und Struktur von TRATON 73

beck-shop.de
DIE FACHBUCHHANDLUNG

II. Compliance bei TRATON 73
B. Problemstellung 74
C. Compliance-Risikoanalyse in der TRATON Gruppe 76
I. Abgrenzung von horizontaler und vertikaler Compliance-Risikoanalyse 76
II. Zusammenspiel mit anderen Risikomanagement-Instrumenten 77
D. Horizontale Compliance-Risikoanalyse 77
I. Zielsetzung 77
II. Vorgehensmodell und Methodik 78
1. Identifikation der relevanten Compliance-Themenfelder 78
2. Identifikation möglicher Governance-Owner 80
3. Analyse der Governance-Strukturen 81
4. Ableitung von Empfehlungen und Berichterstattung 82
E. Vertikale Compliance-Risikoanalyse 82
I. Zielsetzung 82
II. Vorgehensweise und Methodik 83
1. Stufe 1: Top-down-Risikobewertung 83
2. Stufe 2: Bottom-up Risikobewertung 84
3. Berichterstattung, Maßnahmen und Follow-up 85
F. Zusammenfassung 85

§ 5. Compliance-Risikoanalyse im Unternehmen am Beispiel der Siemens AG 86
A. Einführung 86
B. Überblick Compliance Risikoanalyse 87
I. Compliance-Risikoanalyse als Bestandteil eines ganzheitlichen Risikomanagements 87
II. Compliance-Risikoanalyse als wirksame Präventionsmaßnahme des Siemens Compliance Systems 88
1. Integration der Compliance Risikoanalyse in die Geschäftsprozesse 88
2. Was bedeutet der risikobasierte Compliance-Ansatz von Siemens? ... 89
3. Zunehmende Bedeutung der Digitalisierung für das Compliance Risiko Management 89
III. Compliance Risk Assessment zur systematischen Bewertung von Compliance-Risiken 89
IV. Compliance Risk Assessment im weltweiten Siemens Konzern 90
V. Zielsetzung des Compliance Risk Assessments 91
C. Die Unternehmensstruktur von Siemens 92
D. Anwendbarkeit des Compliance Risk Assessment 92
E. Der Prozess für das Compliance Risk Assessment 92
I. Spezieller Ansatz für kartellrechtliche Risiken 93
II. Vorbereitung des Compliance Risk Assessment Workshops 94
1. Datenanalyse aus verschiedenen Quellen und Interviews 94
2. Analyse der erhobenen Daten und Vorbereitung der Workshop-Präsentation 97
3. Vordefinierte Risikobereiche für das Siemens Compliance Risk Assessment 97
III. Management-Workshop zum Compliance Risk Assessment 99
IV. Dokumentation und Weitergabe der Ergebnisse 100
V. Meldung an das Enterprise Risk Management (ERM) 100
VI. Umsetzung der Maßnahmen und Information an alle betroffenen Einheiten 101
F. Erfolgsfaktoren und wichtige Aspekte 101

beck-shop.de
DIE FACHBUCHHANDLUNG

G. Zusammenfassung 101

§ 6. Compliance-Risikoanalyse in mittelständischen Unternehmen des internationalen Maschinen- und Anlagenbaus 102
A. Einleitung 102
B. Begriffsklärungen 102
I. Mittelstand 102
II. Internationaler Maschinen- und Anlagenbau 103
III. Risikomanagement und Risikoanalyse 104
C. Die Risikoanalyse als Grundlage eines Compliance-Management-Systems 104
I. Rechtliche Grundlagen 104
II. IDW Prüfungsstandard 980 105
D. Risikoanalyse in ausgewählten Themengebieten 106
I. Vorbemerkung 106
II. Korruption 107
III. Kartellrecht 109
1. Horizontale Absprachen mit Wettbewerbern 110
2. Vertikale Absprachen mit Nicht-Wettbewerbern, insbes. Lieferanten und Kunden 110
3. Missbrauch einer marktbeherrschenden Stellung 110
IV. Exportkontrolle 111
E. Zusammenfassung und Fazit 113

§ 7. Compliance-Risikoanalyse am Beispiel der öffentlichen Verwaltung 114
A. Einleitung 114
B. Gefährdungsanalyse 115
C. Risikoanalyse 118
D. Sicherungsmaßnahmen 119
E. Zeitplan 119
F. Zusammenfassung 120

beck-shop.de
DIE FACHBUCHHANDLUNG

Kapitel 4. Kartellrechtliche Risikoanalyse

§ 8. Kartellrechtliche Risikoanalyse – Systematik und Aufbau 121
A. Einführung 121
B. Gesetzliche Vorgaben zur kartellrechtlichen Risikoanalyse (§ 130 OWiG) 121
C. Gravierende Sanktionen bei Kartellrechtsverstößen 123
D. Kartellrechtliche Risikoanalyse 124
I. Marktabgrenzung 124
II. Allgemeines Kartellrisiko 125
1. Risikofaktor Marktstruktur 125
2. Risikofaktor Unternehmensstruktur 128
3. Risikofaktor Mitarbeiter 129
III. Konkretes Kartellrisiko 130
1. Berührungspunkte mit Wettbewerbern 130
2. Anlässe zum Tätigwerden 133
E. Risikofaktor Marktmachtmissbrauch 137
F. Organisation der kartellrechtlichen Risikoanalyse 138
G. Ergebnis 139

§ 9. Kartellrechtliche Risikoanalyse – Planung und Umsetzung im Unternehmen 141
A. Einführung 141

B. Notwendigkeit einer kartellrechtlichen Risikoanalyse 141
C. Anreizwirkungen für kartellrechtliche Compliance 142
I. Vermeidung von Kartellrechtsverstößen 142
II. Compliance-Programme als bußgeldmindernder Faktor 143
D. Zuständigkeit für die kartellrechtliche Risikoanalyse („Governance") 144
E. Durchführung der Risikoanalyse 144
I. Konzept der Risikoanalyse 145
II. Kriterien für die Risikoanalyse 146
III. Durchführung der Risikoanalyse 147
IV. Überprüfung und Verifizierung der dezentralen Risikoanalyse 147
V. Risikoanalyse im Rahmen der täglichen kartellrechtlichen Beratung 147
F. Effektive Folgemaßnahmen 148
I. „Tone from the Top/Middle" – Sensibilisierung 148
II. Präsenzschulungen und Schulungsinhalte 149
1. Hardcore-Verstöße 149
2. Sonstige Kartellrechtsverstöße 149
3. Adressaten der Schulungen 150
III. Internet-basierte Schulungen („Web-based trainings") 150
IV. Interne Untersuchungen 151
G. Globalisierung des Kartellrechts – Einheitlichkeit der kartellrechtlichen Beratung? 151
I. Global einheitliche Beratung zu Hardcore-Verstößen 151
II. Nach Ländern differenzierte Beratung zu sonstigen Wettbewerbsbeschränkungen 152

§ 10. Kartellrechtliche Risikoanalyse in mittelständischen Industrieunternehmen – Schwerpunkt Automobilindustrie 153
A. Einleitung 153
I. Risiko mittelständischer Strukturen 153
II. Zielgruppen- und funktionsorientierte Risikobewertung 153
B. Einzelrisiken 154
I. Personalauswahlrisiko 154
1. Fehlendes Erfahrungswissen 154
2. Risikominderung 155
II. Wertschöpfungsstufenrisiko oder: Das Spiel über Bande 156
1. Mehrere Wertschöpfungsstufen im selben Unternehmen 156
2. Der Lieferant als Bote 156
3. Der Kunde als Bote 157
4. Risikominderung 158
C. Kooperationsrisiken in der Automobilindustrie 159
I. Risikobeschreibung 159
II. Arbeitsteilungsrisiko auf Veranlassung des OEM 159
1. Wettbewerber als gemeinsame Lieferanten 159
2. Risikominderung 160
III. Das „Resident Engineer" Risiko 161
1. Alle Wettbewerber unter einem (Kunden-)Dach 161
2. Risikominderung 161
D. Zusammenfassung/Fazit 162

Kapitel 5. Die Prüfung der Compliance-Risikoanalyse aus Sicht der Wirtschaftsprüfer

§ 11. Die Prüfung der Compliance-Risikoanalyse durch den Wirtschaftsprüfer 163
A. Einleitung 163

beck-shop.de
DIE FACHBUCHHANDLUNG

B. Grundlagen zur Prüfung von Compliance-Management-Systemen 165
C. Die Prüfung des Compliance Risk Assessments nach IDW PS 980 166
I. Einordnung in die Systematik des IDW PS 980 166
II. Mögliche Ziele einer Prüfung nach IDW PS 980 167
III. Spezifische Anforderungen an den Wirtschaftsprüfer 168
IV. Prüfungsplanung und Risikobeurteilung des Wirtschaftsprüfers 168
D. Anforderungen an die Compliance-Risikoanalyse 169
I. Anforderungen an das (initiale) Compliance Risk Assessment 169
II. Anforderungen an den Managementprozess für Compliance-Risiken 172
III. Anforderungen an die Dokumentation und Archivierung 172
E. Ausblick 173

Stichwortverzeichnis 175

beck-shop.de
DIE FACHBUCHHANDLUNG