

# Inhaltsverzeichnis

wort. ....	V
zeichnis der Autorinnen und Autoren .....	VII
ürzungsverzeichnis. ....	LIII

## Teil 1

### Grundlagen, Erfolgsfaktoren und Handlungsstrategien

#### 1. Kapitel

#### **Compliance Management – Grundlagen, Orientierungshilfen und Erfolgsfaktoren** (Schulz)

I. Grundlagen und Zusammenhänge. ....	1
1. Anhaltende Bedeutung von Compliance und Compliance Management .....	1
2. Compliance Management als Inbegriff regelkonformer Unternehmensorganisation .....	5
3. Risiken und Nachteile von Regelverletzungen und „Non-Compliance“ .....	7
4. Funktionen von Compliance und Compliance Management. ....	9
5. Compliance Management als Daueraufgabe im dynamischen Umfeld .....	10
6. Compliance als Basis für „Good Corporate Governance“ .....	12
7. Compliance und Reputationsmanagement .....	14
II. Vorgaben und Orientierungshilfen für das Compliance Management .....	15
1. Grundlagen der Compliance-Pflicht – Regelungsbeispiele .....	16
2. Compliance-Pflicht als rechtsformübergreifende Ausprägung der Leitungsverantwortung .....	20
3. Rechtsprechung zur Compliance-Pflicht. ....	21
4. Compliance-Anforderungen anderer Rechtsordnungen. ....	23
a) UK Bribery Act (Vereinigtes Königreich) .....	24
b) Leitfaden des Department of Justice (USA) .....	24
5. Deutscher Corporate Governance Kodex .....	26
6. Erkenntnisse des Risikomanagements .....	26
a) Besonderheiten von Compliance-Risiken .....	27
b) Mögliche Berücksichtigung integrativer Perspektiven .....	28
7. Compliance-Standards als Orientierungshilfe (Beispiel IDW PS 980) .....	29

XVII

III. Erfolgsfaktoren für ein wirksames Compliance Management . . . . .	30
1. Individuelle Konzeption auf Basis des Compliance-Risikoprofils	30
2. Entwicklung einer passenden Compliance-Strategie . . . . .	31
a) Wahl eines unternehmensspezifischen Organisationsmodells	32
b) Klärung von Zuständigkeiten und Delegationsfragen . . . . .	32
c) Fokussierung und Prioritätensetzung bei Compliance-Maßnahmen. . . . .	33
d) Berücksichtigung des besonderen Compliance-Risikoprofils	35
aa) Systematische Identifikation von Compliance-Risiken ..	36
bb) Analyse und Bewertung. . . . .	37
cc) Implementierung von Risikosteuerungsmaßnahmen . . . .	38
dd) Berichterstattung zu Compliance-Risiken . . . . .	38
ee) Durchführung regelmäßiger Compliance-Audits. . . . .	38
3. Förderung und Incentivierung von Regeltreue (Compliance-Kultur) . . . . .	39
aa) Compliance Commitment durch die Unternehmens- und Verbandsleitung . . . . .	40
bb) Akzeptanz als Grundlage der Regelbefolgung . . . . .	41
cc) Kommunikation von Werten und Umgang mit „Regelungslücken“ . . . . .	43
4. Verfassung von Regeln, Richtlinien und Werten. . . . .	44
5. Unabhängige Positionierung der Compliance Officer . . . . .	45
6. Verständliche Schulungen und Fortbildungsprogramme. . . . .	46
a) Bedarfsanalyse und Zielgruppenorientierung . . . . .	46
b) Positionierung von Compliance als „Business Enabler“ . . . . .	47
c) Regelmäßige Anpassung der Fortbildungsformate . . . . .	47
d) Aktive Einbeziehung der Stakeholder . . . . .	47
7. Integration von Compliance-Themen in die Geschäftsprozesse .	48
8. Koordination der Zusammenarbeit mit anderen Unternehmensfunktionen . . . . .	49
9. Einrichtung von wirksamen Kontrollen und Feedback-Prozessen	49
10. Aufklärung von Verstößen und Betrieb von Hinweisgebersystemen. . . . .	50
11. Konsequente Sanktionierung von regelwidrigem Verhalten. . . . .	50
12. „Legal Monitoring“ und regelmäßige Aktualisierung . . . . .	51
13. Angemessene Dokumentation . . . . .	51
IV. Vorteile eines effektiven Compliance Managements . . . . .	51
1. Prävention und Reduzierung der Kostenrisiken und Nachteile von „Non-Compliance“ . . . . .	52
2. Schutz von Unternehmen, Leitungsorganen und Unternehmensangehörigen . . . . .	52
3. Sicherung der Reputation und Vertrauenserhalt der Stakeholder	52
4. Eröffnung und Wahrung rechtlicher Chancen und Gestaltungsoptionen . . . . .	53

5. Vorteile beim Marketing und im Wettbewerb.....	53
6. Verteidigungsmöglichkeiten bei „Non-Compliance“.....	54
7. Verbesserung von Strukturen und Prozessen .....	55
V. Zusammenfassung und Empfehlungen .....	55

## 2. Kapitel

### **Compliance Management und Strafrecht**

(Böttger)

I. Einführung in die Criminal Compliance .....	59
II. Strafrechtliche Grundlagen der Compliance-Verpflichtung .....	67
III. Typische strafrechtliche Compliance-Risiken .....	72
1. Korruption.....	74
a) Vorteilsgewährung (§ 333 StGB).....	77
b) Bestechung (§ 334 StGB) .....	84
c) Bestechung von Mandatsträgern (§ 108e StGB) .....	86
d) Bestechung im geschäftlichen Verkehr (§ 299 Abs. 2 StGB)..	89
e) Bestechlichkeit im geschäftlichen Verkehr (§ 299 Abs. 1 StGB).....	93
f) Bestechung im Gesundheitswesen (§ 299b StGB).....	94
g) Auslandskorruption .....	96
h) Korruptionsdelikte im weiteren Sinne .....	100
2. Untreue (§ 266 StGB) .....	102
a) Generierung von Bestechungsgeld .....	103
b) Zahlung von Bestechungsgeld .....	104
3. Steuerverkürzung (§§ 370 ff. AO) .....	105
IV. Strafrechtliche Risiken der Non-Compliance für die Verantwortlichen des Unternehmens .....	109
1. Originäre strafrechtliche Verantwortlichkeit .....	109
a) Verantwortlichkeit der Geschäftsleitung .....	110
b) Gremienentscheidungen .....	111
c) Delegation von Verantwortungsbereichen.....	112
d) Verantwortlichkeit des Compliance Officers .....	114
e) Aufsichtsrat .....	116
2. Innerbetriebliche Anweisungen/Täterschaft kraft Organisationsherrschaft .....	118
3. Fahrlässigkeitshaftung (sog. Organisationsverschulden).....	119
4. Verletzung der Aufsichtspflicht in Betrieben und Unternehmen (§ 130 OWiG) .....	120

V. Strafrechtliche Risiken der Non-Compliance für das Unternehmen	123
1. (Unternehmens-)Strafrecht	123
a) Überblick	123
b) Einziehung	124
c) Das Unternehmen als Nebenbeteiligter im Strafverfahren	127
2. Ordnungswidrigkeitenrecht	127
a) Verbandsgeldbuße gem. § 30 OWiG	127
b) Das Unternehmen als Nebenbeteiligter im Verfahren wegen § 30 OWiG	130
c) Einziehung (§ 29a OWiG)	130
VI. Sonstige Risiken für das Unternehmen und seine Verantwortlichen	131
1. Blacklisting und Vergabesperren	131
a) Registereintragungen	131
aa) Bundeszentralregister	131
bb) Gewerbezentralregister	131
cc) Vergabe- bzw. Wettbewerbsregister	132
dd) Sonstige Register	134
b) Vergaberechtliche Konsequenzen	135
2. Inhabilität (§§ 70 StGB, 6 GmbHG, 76 AktG)	136
3. Aufsichtsrechtliche Konsequenzen	138
VII. Strafrechtliche Risiken innerhalb des Compliance-Prozesses („Failed Compliance“)	138

3. Kapitel

**Compliance Management als Schnittstellenaufgabe –  
Überlegungen und Empfehlungen zur erfolgreichen Zusammenarbeit  
mit anderen Unternehmensfunktionen**

*(Rau)*

I. Einleitung	143
II. Unternehmensfunktionen und ihre Interaktion im Sinne der Compliance	144
1. Geschäftsleitung	145
2. Aufsichtsrat	149
3. Rechtsabteilung	151
4. Personalabteilung	154
5. Betriebsrat	155
6. Finanzfunktion	157
7. Innenrevision	158
8. Wirtschaftsprüfer	160
9. Unternehmenskommunikation	161
10. Andere	163

11. Von Compliance zu GRC – der Weg zu einer integrierten Governance-, Risiko- und Compliance-Funktion und die Herausforderungen durch ESG .....	164
12. Fallbeispiel .....	165
III. Fazit .....	167

4. Kapitel  
**Einführung eines „Code of Conduct“**  
*(Benkert)*

I. Einleitung .....	171
II. Ausgestaltung .....	172
1. Erscheinungsformen .....	172
2. Typische Regelungen .....	175
III. Einführung eines „Code of Conduct“ .....	177
1. Individualvertragliche Umsetzung .....	178
a) Weisungsrecht des Arbeitgebers .....	178
b) Vertragliche Vereinbarung .....	180
c) Änderungskündigung .....	182
2. Betriebsvereinbarung .....	182
IV. Datenschutzrechtliche Implikation .....	185
V. Mitbestimmungsrecht des Betriebsrats .....	186

5. Kapitel  
**Hinweisgebersysteme – Aufbau und Management**  
*(Block/Sonnenberg)*

I. Einleitung .....	191
1. Begriffsbestimmung .....	193
2. Gründe für die Einführung eines Hinweisgebersystems („Whistleblowing-Systems“) .....	193
3. Aktuelle Rechtliche Rahmenbedingungen .....	195
a) Internationale Anforderungen .....	195
aa) Sarbanes-Oxley Act (SOX) (USA) .....	196
bb) Dodd-Frank Act (USA) .....	196
cc) UK Bribery Act (Großbritannien) .....	197
dd) OECD-Übereinkommen vom 17.12.1997 .....	198
b) Rechtslage in Deutschland .....	199
aa) Gesellschaftsrechtliche Vorgaben .....	200
bb) Ordnungswidrigkeitenrechtliche Vorgaben .....	200
cc) Vorgaben des Deutschen Corporate Governance Kodex ..	201
dd) Vorgaben aus der Rechtsprechung .....	201

II. Die Vorgaben des deutschen Hinweisgeberschutzgesetzes .....	202
1. Ziel des Gesetzes .....	202
2. Überblick über den Inhalt des Hinweisgeberschutzgesetzes ....	203
3. Sachlicher Anwendungsbereich .....	203
4. Persönlicher Anwendungsbereich des Hinweisgeberschutz- gesetzes .....	204
5. Voraussetzungen für den Schutz von Hinweisgebern .....	205
a) Gemeinsame Schutzvoraussetzungen .....	206
b) Besonderheiten in Abhängigkeit vom Meldeweg .....	207
aa) Interne Meldungen gemäß § 17 HinSchG .....	207
bb) Externe Meldungen gemäß § 27 HinSchG .....	208
cc) Offenlegung gemäß § 32 HinSchG .....	209
6. Pflicht zur Einrichtung eines internen Hinweisgebersystems. ....	210
a) Unternehmen des privaten Sektors .....	210
b) Juristische Personen des öffentlichen Sektors .....	211
7. Gesetzliche Anforderungen an ein internes Hinweisgebersystem	211
a) Wahrung der Vertraulichkeit .....	211
b) Meldewege .....	212
c) Interne Meldestelle .....	213
d) Exkurs: Interne Meldestellen im Konzern .....	214
e) Bearbeitung der eingehenden Meldungen .....	215
f) Dokumentation und Datenschutz .....	216
8. Pflicht zur Einrichtung externer Meldestellen .....	217
9. Schutzmaßnahmen .....	219
a) Verbot von Repressalien und Schutz von Hinweisgebern ....	219
b) Sanktionen bei Verstößen .....	221
III. Aufbau/Einführung eines Hinweisgebersystems im Unternehmen .	221
1. Entscheidungen hinsichtlich der konkreten Ausgestaltung. ....	221
a) Organisation .....	221
b) Ausgestaltungsmöglichkeiten .....	222
aa) Kreis der Hinweisgeber .....	222
bb) Zentrale Meldestelle vs. lokale Meldestellen .....	223
cc) Meldekanäle .....	224
dd) Arten der meldbaren Verstöße .....	227
ee) Anonyme Meldungen .....	227
ff) Regelungen zur Einführung eines Hinweisgebersystems .	228
2. Kommunikation .....	229
3. Datenschutzrechtliche Regelungen .....	230
IV. Die praktische Arbeit mit einem Hinweisgebersystem. ....	232
1. Schutz des Hinweisgebers vor Nachteilen .....	232
2. Schutz des Betroffenen. ....	233
3. Datenschutzkonformer Umgang mit eingegangenen Hinweisen.	234
V. Fazit .....	235

6. Kapitel  
**Kommunikationsmanagement und Schulungen**  
**(analog und remote)**  
*(Hastenrath)*

I. Einleitung.....	237
II. Grundzüge zur Kommunikation in der Unternehmenspraxis .....	238
1. Relevanz der Kommunikation im Unternehmen und bei Compliance .....	238
2. Kommunikationsmodelle .....	240
a) Modell zu Konfliktarten als Grundlage für die Kommunikation .....	240
b) Praxisrelevantes Beispiel .....	242
III. Ausgewählte Instrumente der Compliance-Kommunikation.....	245
1. Tone from the Top .....	245
2. Persönlicher Kontakt mit dem Compliance Officer .....	246
3. Zusammenarbeit des Compliance Officers mit Schlüsselfunktionen im Unternehmen.....	246
4. Schriftliche Informationen an die Mitarbeiter .....	247
5. Compliance im firmeneigenen Intranet.....	247
IV. Schulungen .....	248
1. Persönliche Schulungen durch die Compliance-Funktion.....	248
2. Schulungen mit klassischem E-Learning .....	249
3. Digitale Schulungen: Schulungen mit Webinaren, Podcasts, Livestreams oder vertonten Präsentationen .....	250
4. Unterstützung dezentraler Compliance-Funktionen: das Schulungshandbuch .....	263
V. Die „Top 5 Stolpersteine“ in der Compliance-Kommunikation und Lösungsvorschläge.....	265
1. Fehlende, verspätete oder missverständliche Information.....	265
a) Problemstellung .....	265
b) Lösungsvorschlag.....	266
2. Mangelnde Authentizität („Nicht gelebte Hochglanzaussagen“). .....	267
a) Problemstellung .....	267
b) Lösungsvorschlag.....	267
3. Fehler im Kommunikationsmanagement: Budget- und Ressourcenmangel.....	268
a) Problemstellung .....	268
aa) Unzureichende Übersetzung eines Code of Conduct (CoC).....	269
bb) Unzureichendes Schulungsbudget.....	270
b) Lösungsvorschlag.....	271

4. Probleme mit der Technik .....	271
a) Problemstellung .....	271
b) Lösungsvorschlag .....	272
5. Fehler im Kommunikationsmanagement von Compliance aufgrund von Kulturunterschieden .....	274
a) Problemstellung .....	274
b) Lösungsvorschlag .....	275
VI. Fazit zur Compliance-Kommunikation .....	276

7. Kapitel

**Auswirkungen des ISO-Standards 37301 auf  
die Prüfung von Compliance-Management-Systemen  
nach IDW PS 980 und Vergleich mit ISO 31022**

*(Uhlig/Federmann)*

I. Einleitung .....	279
II. Zielsetzung und Zielgruppe .....	280
1. Ausgangslage .....	280
2. Zielsetzung des IDW PS 980 .....	281
3. Zielsetzung des ISO 37301:2021 .....	281
4. Vergleich .....	282
III. Unterschiedliche Regelungstiefe zur Ausgestaltung des CMS .....	282
1. CMS-bezogene Regelungsinhalte des IDW PS 980 .....	282
2. Regelungsinhalte des ISO 37301 .....	283
IV. ISO 37301 als geeignetes, angemessenes Rahmenkonzept für ein CMS .....	286
1. Anforderungen des IDW PS 980 an ein Rahmenkonzept .....	286
2. Vergleich ISO 37301 Anforderungen mit IDW PS 980-Grundelementen .....	287
V. Zwischenergebnis .....	289
VI. Die Legalitätskontrolle als Bindeglied zwischen Risiko- und Compliance-Management? .....	289
1. Zielsetzung des ISO 31022 .....	291
2. Regelungsinhalte des ISO 31022 .....	291
3. Vergleich zum Compliance-Risiko/Vergleich zur ISO 37301 ...	292
4. Zwischenergebnis .....	292
VII. Argumente für eine Ausrichtung des CMS nach ISO 37301 .....	293
1. Basis für Ermessensentscheidung und Compliance-Richtlinie ..	293
2. Beurteilung der angemessenen Einrichtung eines wirksamen CMS .....	295
VIII. Zusammenfassung .....	296



8. Kapitel  
**Management interner Untersuchungen**  
*(Wettner/Walter)*

I. Einleitung.....	299
II. Entscheidung über die Durchführung interner Untersuchungen....	300
1. Entscheidungsbefugte Stellen.....	301
2. Pflicht zur Aufklärung konkreter Verdachtsfälle.....	301
3. Interne Untersuchung oder externe Ermittlung?.....	302
a) Bereits laufendes behördliches Verfahren.....	303
b) (Noch) kein behördliches Verfahren.....	304
III. Vornahme von Eilmaßnahmen.....	305
1. Einrichtung einer zentralen Koordinierungsstelle.....	306
2. Maßnahmen der Daten- und Beweissicherung.....	306
3. Arbeitsrechtliche Maßnahmen.....	307
4. Beachtung von Informations- und Berichtspflichten.....	307
IV. Planung der internen Untersuchung.....	308
1. Grundlagen der Planung.....	308
a) Beachtung von Recht- und Verhältnismäßigkeit.....	308
b) Beachtung von Risiken und Folgen der internen Untersuchung.....	309
2. Festlegung des Untersuchungsgegenstands.....	310
3. Bestimmung des Untersuchungsteams und der Verantwortlichkeiten.....	311
a) Auswahl von Mitarbeitern und externen Beratern.....	311
b) Festlegung von Verantwortlichkeiten und Berichtswegen....	312
4. Bestimmung und Vorbereitung der Informationsquellen.....	313
a) Relevante Informationsquellen.....	313
aa) Dokumente.....	313
bb) Elektronische Daten und E-Mails.....	313
cc) (Ehemalige) Mitarbeiter.....	314
b) Notwendige Abstimmung der geplanten Untersuchungsmaßnahmen.....	315
aa) Beteiligung von Betriebsrat oder Sprecherausschuss.....	315
bb) Abstimmung mit Ermittlungs- und Aufsichtsbehörden...	315
c) Einrichtung eines Datenraums oder eines „Projektportals“...	316
5. Sicherung der Vertraulichkeit.....	317
a) Zugriffsmöglichkeiten Dritter.....	317
aa) Beschlagnahme durch Ermittlungsbehörden.....	317
bb) Herausgabe von Unterlagen an Versicherer.....	319
b) Begrenzung der E-Mail- und sonstigen schriftlichen Kommunikation.....	319

c) Kennzeichnung und Aufbewahrung geschützter Kommunikation .....	320
6. Erstellen eines Untersuchungsplans .....	321
V. Durchführung der internen Untersuchung .....	321
1. Allgemeine Untersuchungsgrundsätze .....	321
2. Dokumentation der Untersuchung .....	322
3. Erhebung und Auswertung von Dokumenten .....	323
4. Erhebung und Auswertung von elektronischen Daten .....	324
5. Befragung von Mitarbeitern .....	324
6. Auswertung und Aufarbeitung der Untersuchungsergebnisse ...	326
VI. Fazit .....	328

Teil 2

**Übergreifende Themen und Herausforderungen**

Abschnitt 2.1

**Risiko und Governance**

9. Kapitel

**Risiko- und Chancenmanagement –  
Erfolgsfaktoren für eine wirksame Umsetzung**

*(Romeike)*

I. Corporate Governance und das Management von Chancen und Risiken .....	331
1. Grundlagen und Einführung .....	331
2. Die Odyssee und der Umgang mit Risiken .....	333
3. Risikomanagement als zentraler Erfolgsfaktor .....	335
4. Überblick über aktuelle regulatorische Entwicklungen .....	335
5. Krisenfrüherkennung gemäß Unternehmensstabilisierungs- und -restrukturierungsgesetz (StaRUG) .....	336
6. FISG fordert Internes Kontrollsystem und Risikomanagement- system .....	338
II. Abgrenzung des Risiko- und Chancenbegriffs .....	339
III. Nutzen eines wirksamen Chancen- und Risikomanagements .....	342
IV. Unterscheidung von Ursachen – Risiken – Wirkungen .....	344
V. Verknüpfung von Risikomanagement und Strategie .....	347
VI. Der Risikomanagement-Prozess als Regelkreis .....	349

VII. Methoden zur Risikoidentifikation und -bewertung .....	353
VIII. Aggregation von Risiken .....	356
IX. Maßnahmen zur Risikosteuerung .....	357
X. Unterschiedliche Reifegrade im Risikomanagement .....	360
XI. Fazit und Ausblick .....	361

## 10. Kapitel

### **Auditverfahren: Compliance als Dauerpflcht**

*(Rack)*

I. Einleitung .....	367
II. Die Dauerpflcht zur Sicherstellung der dauerhaften Wirksamkeit des CMS nach DIN und EMAS .....	367
III. Die Beweislast für Vorstände und Geschäftsführer .....	369
IV. Die Unvorhersehbarkeit von Rechtsverstößen als Grund für Compliance als Dauerpflcht .....	369
V. Zertifikate sind bloße Momentaufnahmen ohne Nachweis dauerhafter Wirksamkeit eines CMS .....	369
VI. Das Stichprobenargument in Rechtsprechung und Literatur .....	370
VII. Der erfolglose Entlastungsversuch durch den Hinweis auf Regeln ohne Anwendung .....	372
VIII. Die Haftung von Vorständen und Geschäftsführern für fehlende und fehlerhafte CMS nach der Rechtsprechung .....	375
IX. Die Haftung von Auditoren und Umweltgutachtern gegenüber dem zertifizierten Unternehmen nach der Expertenhaftung .....	375
X. Die Expertenhaftung von Auditoren und Umweltgutachtern gegenüber Dritten .....	377
XI. Aufsicht und Sanktionen von Behörden gegen Umweltgutachter und Auditoren für falsche Zertifikate nach dem Auditverfahren ...	378
XII. Der Gesetzeszweck des UAG .....	378
XIII. Die Zulassung .....	378
XIV. Die Aufsicht .....	379

XV. Die Konkretisierung des UAG durch Richtlinien des Umweltgutachterausschusses.....	379
XVI. Mehr Risiken durch Anordnungen, Untersagungen und Widerruf der Zulassung für Umweltgutachter und Auditoren durch Hinweise auf Rechtsverstöße nach dem Hinweisgeberschutzgesetz .....	380
XVII. Mehr Risiken für Umweltgutachter und Auditoren durch den erweiterten Kreis der Hinweisgeber außerhalb der Unternehmensbelegschaft.....	381
XVIII. Fazit .....	382

## 11. Kapitel

### **Governance, Risk und Compliance im Mittelstand – Zusammenhänge und Abhängigkeiten**

*(Bartuschka)*

I. Einleitung – Die Notwendigkeit der Einrichtung von Instrumenten zur Überwachung von Unternehmen .....	383
II. Das System der Unternehmensüberwachung .....	386
1. Überblick über das Gesamtsystem.....	386
2. Externe Komponenten der Unternehmensüberwachung .....	386
3. Interne Komponenten der Unternehmensüberwachung.....	388
III. Die Verknüpfung der einzelnen Elemente der Unternehmensüberwachung.....	389
1. Der GRC-Ansatz .....	389
2. Das interne Kontrollsystem und die anderen Elemente der Überwachung des Unternehmens.....	390
3. Compliance- und Risikomanagement .....	391
4. Risikomanagement und Controlling .....	392
5. Interne Revision, Compliance und Risikomanagement.....	393
6. Fazit .....	393
IV. Grundkonzept für die Ausgestaltung eines integrierten Systems der Überwachung für mittelständisch geprägte Unternehmen.....	394
1. Bestimmung der Zielgruppe der Unternehmen.....	394
2. Zielstellung für die Einführung eines integrierten Systems der Überwachung .....	394
3. Vorgehensweise .....	394
a) Risikoanalyse .....	395
b) Analyse bestehender Strukturen .....	396
c) Ermittlung des Anpassungsbedarfs .....	396
d) Umsetzung.....	397
4. Fazit .....	399

Abschnitt 2.2

**Datenschutz und IT-Security**

12. Kapitel

**Datenschutz im Compliance Management**

*(Becker/Böhlke/Fladung)*

I. Einleitung.....	401
II. Der konzeptionelle Schutz personenbezogener Daten .....	405
1. Gesetzliche Grundlagen .....	405
a) Datenschutzgrundverordnung .....	405
b) Bundesdatenschutzgesetze .....	406
c) Landesdatenschutzgesetz .....	406
d) Europäische Richtlinien und Verordnungen .....	407
e) Weitere Gesetze mit datenschutzrechtlichen Vorgaben.....	408
2. Zentrale Grundsätze .....	409
a) Verbot mit Erlaubnisvorbehalt.....	409
b) Prinzip der Verhältnismäßigkeit .....	412
c) Datensparsamkeit .....	412
d) Transparenz .....	413
e) Zweckbindung.....	413
3. Grundbegriffe .....	413
a) Personenbezogene Daten.....	414
b) Verantwortliche Stelle .....	415
c) Umgang mit personenbezogenen Daten.....	415
aa) Erheben .....	416
bb) Speichern .....	416
cc) Verändern .....	416
dd) Übermitteln.....	416
d) Auftragsverarbeitung.....	419
III. Betrieblicher Datenschutz.....	420
1. Pragmatischer Ansatz: Wo fange ich an? .....	420
2. Beratungspraxis .....	425
a) Der betriebliche Datenschutzbeauftragte.....	428
b) Prozess der Datenschutzberatung .....	430
c) Praxisrelevante Beispiele .....	433
3. Implementierung .....	435
4. Zusammenarbeit mit Behörden.....	438
IV. Instrumente der datenschutzrechtlichen Compliance .....	439
1. Tone from the Top .....	439
2. Interne Richtlinien.....	439
a) Datenschutzrichtlinie.....	440

b) IT-Nutzungsrichtlinie .....	440
c) E-Mail-Policy .....	441
d) Social-Media und Messaging-Dienste .....	442
e) IT-Datenschutzmanagement-Richtlinie (Datenschutzmanagementkonzept) .....	442
f) Archivierungs- und Löschungsrichtlinie .....	443
3. Verzeichnis von Verarbeitungstätigkeiten .....	444
4. Interne Kommunikation und Awareness .....	445
a) Der Datenschutz-Newsletter .....	445
b) Intranet .....	446
c) Der „Datenschutz-Tag“ und Fachtagungen .....	446
5. Schulungen .....	446
a) Persönliche Schulungen .....	447
b) E-Learning/Webinars .....	448
c) Unterstützung dezentraler Compliance-Funktionen .....	449
V. Effektive Datenschutzüberwachung .....	450
1. Audits und Maßnahmenpläne/Quick Self-Assessment .....	450
2. IT-Infrastruktur-Reviews und Koordinierung mit IT-Security ...	452
3. Incident- und Regel-Reporting aus den Betrieben .....	452
4. Der Datenschutzjahresbericht .....	453
5. Bericht an Aufsichtsrat/Compliance-Bericht/Audit Committee .	453
6. Zusammenarbeit mit dem Compliance Officer, IT-Security und Revision .....	454
VI. Beschäftigtendatenschutz .....	457
1. Bedeutung des Beschäftigtendatenschutzes für Compliance ....	457
2. Rechtsgrundlagen für den Umgang mit Mitarbeiterdaten .....	461
a) Kollektivvereinbarungen zur Nutzung von Mitarbeiterdaten .	461
b) Rechtfertigende Einwilligung des Mitarbeiters .....	463
c) Arbeitsvertragliche Regelungsmöglichkeiten .....	464
d) Gesetzliche Erlaubnistatbestände .....	466
e) Internationaler Datenverkehr mit Beschäftigtendaten .....	469
3. Risiken beim Umgang mit Beschäftigtendaten .....	470
a) Phase 1: Begründung des Arbeitsverhältnisses/ „Boarding-Phase“ .....	471
b) Phase 2: Durchführung des Arbeitsverhältnisses/ „On Board-Phase“ .....	471
c) Phase 3: Beendigung des Arbeitsverhältnisses/ „Off Boarding-Phase“ .....	472
4. Zusammenarbeit mit dem Betriebsrat .....	473
5. Personalleiter und Betriebsrat als Teil des Datenschutz- und Compliance-Teams .....	475
6. Hinweise, Muster und Beispielsfall .....	476
a) Hinweise zur Regelung der Nutzung von Beschäftigtendaten	476

b) Hinweise zur Regelung der Nutzung von Internet und E-Mail	478
c) Beispielsfall zur Kontrolle bei Verdacht gegen Mitarbeiter...	481
d) Beispielsfall zum Auskunftsrecht eines Mitarbeiters bei Untersuchungen von Compliance-Verstößen .....	483
VII. Fazit.....	485

### 13. Kapitel

## **IT-Compliance – Software-Lizenzmanagement, Blockchain und Nutzung von Daten**

*(Jacobs)*

I. Rechtliche Herausforderungen der fortschreitenden Digitalisierung und Vernetzung .....	487
II. Software-Lizenzmanagement.....	487
1. Rechtliche Grundlagen der Nutzung von Computerprogrammen	488
2. Besondere Arten von Software, insbesondere Open-Source-Software .....	489
3. Software-Lizenzmanagement im Rahmen verantwortungs- bewusster Unternehmensführung .....	490
4. Rechtsfolgen einer Unterlizenzierung .....	491
III. Software-Lizenzmanagement im Rahmen von Cloud-Diensten ....	491
1. Nutzungshandlungen beim Cloud Computing .....	491
a) Recht der öffentlichen Zugänglichmachung der Software ....	492
b) Recht zur Vervielfältigung der Software .....	493
2. Lizenzmanagement im Zusammenhang mit Cloud Computing- Diensten .....	493
IV. Rechtsrahmen von Softwarelizenz-Audits.....	494
1. Rechtliche Grundlagen für einen Softwarelizenz-Audit .....	495
2. Vertragliche Ausgestaltung eines Softwarelizenz-Audits .....	496
V. Rechte an und Zugang zu nicht-personenbezogenen Daten.....	497
1. Regelungsinhalt und Struktur des Data Act .....	499
2. Datenweitergabe unter dem Data Act .....	500
a) Allgemeine Pflichten .....	501
b) Erfasste Datenkategorien .....	502
c) Datenzugriffsrechte für Nutzer .....	502
d) Recht der Nutzer auf Datenweitergabe an Dritte .....	503
3. Verhältnis zum Datenschutzrecht .....	504
4. Nutzung durch und Weitergabe von Daten durch den Dateninhaber.....	504
5. Missbräuchliche Vertragsklauseln .....	506
6. Sanktionen.....	506

VI. Wechsel von Datenverarbeitungsdiensten.....	507
VII. Blockchain und Smart Contracts .....	508
VIII. Implementierung eines IT-Compliance-Systems.....	509

14. Kapitel

**Cybersecurity, IT-Sicherheit und Krisenmanagement**

*(Bensinger)*

I. Analyse .....	511
1. Ziele der IT-Sicherheit .....	511
2. Cybercrime im Wandel .....	512
a) Ideelle Hintergründe .....	513
b) Materielle Hintergründe .....	516
3. Entwicklungen bei Schutzmaßnahmen.....	516
II. Vorbeugende Maßnahmen .....	517
1. Adressaten .....	518
a) KRITIS-Betreiber .....	518
b) Anbieter von Telemediendiensten .....	520
c) Anbieter von Telekommunikationsdiensten .....	521
d) Bank- und Finanzwesen .....	522
e) Energiewirtschaft.....	522
f) Geschäftsführung von Aktiengesellschaften und GmbHs ....	523
2. Inhalt der gesetzlichen Verpflichtungen .....	523
a) BSIG.....	525
aa) Pflichten der KRITIS-Betreiber.....	525
bb) Befugnisse des BSI.....	527
b) KRITIS-Dachgesetz .....	528
c) DSGVO .....	529
d) BDSG.....	535
e) TTDSG und TKG.....	535
aa) TTDSG.....	535
bb) TKG.....	535
cc) Verhältnis zur DSGVO .....	536
f) KWG, ZAG, MaRisk etc.....	537
aa) MaRisk (Mindestanforderungen an das Risikomanagement) .....	538
bb) ZAG.....	542
cc) § 27 Abs. 1 ZAG .....	544
dd) DORA.....	544
ee) Konkurrenz zum BSIG .....	545
g) EnWG.....	545
h) NIS-Richtlinien .....	546



i) §§ 76, 91, 93 AktG .....	547
aa) Ausgestaltung des IT-Risikomanagementsystems .....	548
bb) Anforderungen nach DSGVO .....	551
cc) Verantwortungsverteilung innerhalb der Geschäftsleitung .....	552
dd) Dokumentationspflicht .....	553
3. Unternehmensinterne Vorkehrungen .....	553
a) Interne Vorgaben .....	553
b) Aktuelle technisch-organisatorische Schutzmaßnahmen .....	554
III. Der Krisenfall .....	556
1. Hacker-Angriffe erkennen .....	556
2. Rechtliche Konsequenzen und Handlungsoptionen .....	556
a) Melde- und Informationspflichten .....	556
aa) DSGVO .....	556
(1) Meldung an die Aufsichtsbehörde (Art. 33 DSGVO) .....	557
(2) Meldung an die Betroffenen (Art. 34 DSGVO) .....	559
(3) Sanktionen .....	562
bb) BDSG .....	562
cc) BSIG .....	562
dd) ZAG .....	564
ee) Meldepflichten für Energiewirtschaftsunternehmen .....	566
ff) TMG .....	566
gg) TKG .....	567
hh) Sonstige Informationspflichten .....	568
b) Werkzeuge zur Abwehr von Cyberangriffen .....	568
3. Interne und externe Kommunikation .....	570
4. Mittel- und längerfristige Maßnahmen .....	570
IV. Ausblick .....	571

## Abschnitt 2.3

### ESG und Governance

#### 15. Kapitel

### **Corporate Social Responsibility und Corporate Compliance – Entwicklungslinien gesellschaftlicher und juristischer Verantwortung von Unternehmen**

*(Stehr/Knopp)*

I. Einleitung .....	573
1. „Shareholder Value“ und „Stakeholder Value“ – eine „Mission Impossible“ für Unternehmen? .....	573
2. CSR und Unternehmensführung – Auswirkungen auf die Unternehmen? .....	575
3. CSR und Unternehmensführung – Wechselwirkungen mit dem Compliance Management .....	576

<b>II. Grundlagen</b> .....	<b>577</b>
1. Corporate Social Responsibility.....	577
a) Bedeutungswandel des Begriffsverständnisses .....	577
b) Konzeptionen und Modelle .....	577
c) Definitionen .....	579
2. Corporate Governance .....	581
a) Begriffsverständnis .....	581
b) Corporate Governance und Corporate Social Responsibility .	581
c) Gesellschaftsrecht und Deutscher Corporate Governance Kodex .....	583
3. Corporate Compliance .....	585
a) Begriffsverständnis .....	585
b) Corporate Compliance und Corporate Governance .....	586
c) Corporate Compliance als Organisationspflicht .....	587
d) Aktuelle gesetzliche Entwicklungen in Deutschland und der Europäischen Union .....	588
<b>III. Corporate Social Responsibility und Regulierungsebenen</b> .....	<b>590</b>
1. Einführung in die CSR-Regulierung .....	590
a) Regulierungsebenen .....	590
b) Regulierungsansätze .....	590
c) Rechtsqualität .....	591
d) Reputationsmanagement .....	592
2. Beispiele für CSR-Regulierung .....	592
a) Globale Regulierungsebene.....	592
aa) OECD-Leitsätze für multinationale Unternehmen .....	592
bb) GRI-Berichtsstandards .....	593
cc) UN Global Compact.....	594
dd) ISO 26000 .....	595
b) Internationale Regulierungsebene .....	596
c) Supranationale bzw. europäische Regulierungsebene .....	597
d) Nationale bzw. deutsche Regulierungsebene .....	597
3. CSR-Normenflut als Herausforderung für Unternehmen .....	599
<b>IV. Corporate Social Responsibility und Corporate Compliance</b> .....	<b>601</b>
1. Einführung .....	601
2. Allgemeine Relevanz von CSR-Normen für die Corporate Compliance.....	603
3. Konkrete Relevanz von CSR-Normen sowie sonstiger CSR-Themen für die Corporate Compliance.....	604
a) CSR-Normen und CSR-Themen im Compliance- Risikomanagementprozess.....	605
aa) Schritt 1: Definition der Compliance-Risiken .....	605
bb) Schritt 2: Identifikation der Compliance-Risiken .....	605

cc) Schritt 3: Analyse und Bewertung der Compliance-Risiken.....	606
dd) Schritt 4: Berichterstattung der Compliance-Risiken ....	607
ee) Schritt 5: Steuerung der Compliance-Risiken .....	607
ff) Schritt 6: Monitoring der Compliance-Risiken.....	608
b) Verknüpfung von CSR- und Compliance-Risiken .....	608
V. Zusammenfassung .....	608

## 16. Kapitel

### **„ESG-Compliance“:**

### **Herausforderungen des Nachhaltigkeitsreportings**

(Beisheim)

I. Einleitung: Nachhaltigkeit, Corporate Governance und die Rolle von Compliance.....	611
II. Status quo und bald Historie: Die CSR-Richtlinie und das CSR-Richtlinie-Umsetzungsgesetz von 2017.....	614
1. Zielsetzungen der CSR-Richtlinie und des CSR-Richtlinie-Umsetzungsgesetzes .....	614
2. Neuausrichtung des Nachhaltigkeitsreportings .....	615
a) Bereits vor dem CSR-RUG vorhandene nichtfinanzielle Berichtspflichten im deutschen Bilanzrecht .....	616
b) Sog. Soft-Law-Ansätze als Rahmenwerke für das CSR-Reporting .....	617
c) Paradigmenwechsel .....	618
3. Adressaten der CSR-Berichtspflichten nach dem CSR-RUG....	619
4. Berichtsansforderungen im Rahmen des Reportings nach der bislang geltenden CSR-Richtlinie .....	621
a) Berichtsvarianten: Die nichtfinanzielle Erklärung und der gesonderte Bericht .....	621
b) Inhalte, Relevanzmaßstab und Methodik des CSR-Reportings	623
c) Muster: Struktur und Ansätze zur Gestaltung des CSR-Reportings .....	626
d) Die Möglichkeit der Verwendung von Rahmenwerken .....	629
5. Nichtangaben, unrichtige Angaben und ihre Folgen.....	631
a) Der „Comply or Explain“-Grundsatz .....	631
b) Ein Sonderfall: Das (vorübergehende) Weglassen nachteiliger Angaben .....	632
c) Prüfungen.....	633
d) Verstöße, Säumnisse und Sanktionen .....	635
III. Die CSRD: Neue Anforderungen im Nachhaltigkeitsreporting ....	636
1. Adressaten und Konzernprivileg.....	640

2. Überblick über die ESRS .....	642
a) Regelungsinhalte des Set 1 der ESRS .....	643
b) Der Grundsatz der doppelten Wesentlichkeit und weitere Verfahrensvorgaben .....	647
c) Verortung im Lagebericht und Prüfung .....	651
d) Erleichterungen im Rahmen der Implementierung des Reportings .....	652
IV. Der Referentenentwurf zum CSRD-Umsetzungsgesetz und ein weitergehender Ausblick .....	653

17. Kapitel

**Compliance im Kontext nachhaltigen Supply Chain Managements –  
Die betriebswirtschaftliche Perspektive**

*(Schleper/Förstl)*

I. Einleitung .....	659
II. Nachhaltiges Lieferantenmanagement .....	661
1. Lieferantenbewertung .....	661
2. Lieferantenentwicklung .....	662
3. Lieferantenauswahl .....	663
4. Lieferantenmonitoring .....	663
III. Unterschiede entlang der Lieferkette .....	664
IV. Menschenrechtsprobleme und Due Diligence – „beyond compliance“ .....	666
V. Praxisrelevanz .....	669
VI. Fazit .....	670

18. Kapitel

**Lieferkettensorgfaltspflichtengesetz (LkSG) – Einführung und praktische  
Hinweise zur Umsetzung der Sorgfaltspflichten im Unternehmen**

*(Heske)*

I. Wesentliche Regelungen des LkSG im Überblick .....	671
1. Entstehung, Zielsetzung und Anwendungsbereich .....	671
2. Definition der Lieferkette .....	672
a) Lieferkette nach § 2 Abs. 5 LkSG .....	672
b) Erfasste Handlungsbereiche im Rahmen der Lieferkette .....	673
3. Menschenrechtliche und umweltbezogene Risiken und Pflichten .....	675
a) Menschenrechtliche Risiken .....	676
b) Umweltbezogene Risiken .....	676
c) Menschenrechtsbezogene und umweltbezogene Pflichten ...	677

<b>II. Praktische Hinweise zur Umsetzung der Sorgfaltspflichten im Unternehmen .....</b>	<b>677</b>
1. Verantwortlichkeiten im Rahmen der Einhaltung der Sorgfaltspflichten.....	677
2. Sorgfaltspflichten im Unternehmen nach dem LkSG.....	678
a) Synergien erkennen – Compliance-Management-System nutzen .....	679
b) Umsetzungsprojekt: Vorüberlegungen zur Implementierung der Sorgfaltspflichten.....	679
c) Die Sorgfaltspflichten im Überblick.....	681
aa) Angemessenes und wirksames Risikomanagement (§ 3 Abs. 1 Nr. 1 LkSG) .....	682
bb) Festlegung einer betriebsinternen Zuständigkeit (§ 3 Abs. 1 Nr. 2 LkSG) .....	684
cc) Risikoanalyse (§ 3 Abs. 1 Nr. 3 LkSG) .....	685
(1) Ziele der Risikoanalyse .....	685
(2) Bedeutung der Risikoanalyse und Vorüberlegungen .	685
(3) Umfang und Inhalt der Risikoanalyse.....	686
(4) Regelmäßige und anlassbezogene Risikoanalyse ....	689
(5) Unternehmensinterne Kommunikation der Risikoanalyse .....	690
dd) Abgabe einer Grundsatzerklärung (§ 3 Abs. 1 Nr. 4 LkSG) .....	690
ee) Verankerung von Präventionsmaßnahmen (§ 3 Abs. 1 Nr. 5 LkSG) .....	692
(1) Präventionsmaßnahmen im eigenen Geschäftsbereich (§ 6 Abs. 3 LkSG) .....	692
(2) Präventionsmaßnahmen gegenüber unmittelbaren Zulieferern (§ 6 Abs. 4 LkSG) .....	693
(3) Wirksamkeit und Aktualisierung der Präventionsmaßnahmen (§ 6 Abs. 5 LkSG).....	696
ff) Abhilfemaßnahmen (§ 3 Abs. 1 Nr. 6 LkSG).....	696
(1) Abhilfemaßnahmen im eigenen Geschäftsbereich (§ 7 Abs. 1 LkSG) .....	696
(2) Abhilfemaßnahmen bei einem unmittelbaren Zulieferer (§ 7 Abs. 2 LkSG).....	697
(3) Wirksamkeit und Aktualisierung der Abhilfemaßnahmen (§ 7 Abs. 4 LkSG).....	698
gg) Einrichtung eines Beschwerdeverfahrens (§ 3 Abs. 1 Nr. 7 LkSG) .....	698
hh) Risiken bei mittelbaren Zulieferern (§ 3 Abs. 1 Nr. 8 LkSG) .....	700

(1) Substantiierte Kenntnis (§ 9 Abs. 3 LkSG) .....	700
(2) Maßnahmen nach Erlangung von substantiierte Kenntnis (§ 9 Abs. 3 LkSG) .....	701
ii) Dokumentation und Berichterstattung (§ 3 Abs. 1 Nr. 9 LkSG) .....	702
(1) Dokumentationspflichten (§ 10 Abs. 1 LkSG) .....	702
(2) Berichtspflicht (§ 10 Abs. 2 LkSG) .....	702
III. Das BAFA als zuständige Behörde für die Kontrolle und Durchsetzung der Regelungen des LkSG .....	703
1. FAQs, Handreichungen und sonstige Informationsquellen .....	703
2. Berichtspflicht und Kontrollen .....	704
a) Elektronische Berichtspflicht der Unternehmen .....	704
b) Kontrollbefugnisse des BAFA .....	705
c) Anordnungen und Maßnahmebefugnisse des BAFA .....	706
IV. Sanktionen .....	706
1. Bußgeld und Bemessungsgrundlage .....	707
2. Ausschluss von der Vergabe öffentlicher Aufträge .....	707
V. Zivilrechtliche Haftung und Prozessstandschaft .....	708
VI. Auswirkungen der europäischen Lieferkettenregelung (CSDDD) – Anpassung des LkSG .....	708

19. Kapitel

**Menschenrechtsbeauftragte und  
Beschwerdebeauftragte nach dem LkSG**  
*(Hagel/Wiedmann)*

I. Einleitung .....	711
II. Menschenrechtsbeauftragte .....	711
1. Begrifflichkeiten und gesetzliche Grundlagen .....	711
2. Überwachungsaufgaben .....	713
3. Anforderungen an Menschenrechtsbeauftragte .....	715
a) Qualifikation .....	715
b) Unparteilichkeit, Unabhängigkeit und Weisungsungebundenheit .....	716
c) Verschwiegenheit .....	717
4. Ernennung .....	718
5. Stellung im Unternehmen .....	718
6. Arbeitsrechtlicher Schutz .....	721
7. Auslagerung der Funktion .....	721
8. Haftung .....	722

III. Beschwerdebeauftragte .....	723
1. Begrifflichkeiten und gesetzliche Grundlagen.....	723
2. Aufgaben .....	724
3. Anforderungen an Beschwerdebeauftragte.....	726
a) Qualifikation .....	726
b) Unparteilichkeit, Unabhängigkeit und Weisungsungebundenheit .....	727
c) Verschwiegenheit .....	728
4. Ernennung .....	728
5. Stellung im Unternehmen.....	728
6. Arbeitsrechtlicher Schutz.....	729
7. Haftung .....	729
8. Abgrenzung zum Meldestellenbeauftragten nach HinSchG .....	729
IV. Verhältnis Menschenrechts- zu Beschwerdebeauftragtem .....	730
V. Fazit.....	731

### Teil 3

## Besondere Aufgaben und Anwendungsfelder

### 20. Kapitel

## Die Compliance-Funktion in einem Kreditinstitut

*(Renz/Frankenberger)*

I. Einleitung: Was ist die Bedeutung des Begriffs Compliance?.....	733
II. Welche Compliance-Funktionen gibt es in einem Kreditinstitut?..	734
1. Kapitalmarkt-Compliance .....	735
2. Zentrale Stelle/sonstige strafbare Handlungen (inkl. Geldwäscheprävention) sowie Finanzsanktionen und Embargo (Anti-Financial Crime (AFC)).....	739
3. MaRisk-Compliance .....	742
4. Hinweisgebersystem (Whistleblowing).....	744
5. Datenschutz.....	746
6. Auslagerung der Compliance-Funktion oder von einzelnen Compliance-Tätigkeiten.....	748
III. Inhalt und Aufgabe einer modernen Compliance-Funktion.....	749
IV. Das Compliance-Management-System (CMS) .....	750
V. Schnittstellen zu anderen Funktionen.....	754
1. Fachbereiche .....	755
2. Rechtsbereich .....	755
3. Risikocontrolling-Funktion .....	757
4. Interne Revision .....	757

VI. Compliance als Teil des IKS eines Kreditinstituts. ....	759
VII. Übertragung der Struktur/des Ansatzes auf andere Industriesäulen – und umgekehrt .....	764
VIII. Fazit/Ausblick. ....	766
21. Kapitel	
<b>Produktbezogenes Compliance- und Risikomanagement im Treasury</b>	
<i>(Keßler)</i>	
I. Einleitung .....	767
II. Finanz- und Kapitalmarktprodukte; Risiken .....	768
1. „Einfache“ Produkte .....	768
2. „Komplexe“ Produkte. ....	769
a) Überblick .....	769
b) Risiken im Einzelnen .....	772
III. Rechtliche Anforderungen an das Risikomanagement- und Compliance-System .....	774
1. Anforderungen an Finanzinstitute .....	774
a) Aufsichtsrechtliche Anforderungen .....	774
b) „Best Practice“ und praktische Ausgestaltung .....	776
aa) Risikomanagement. ....	776
(1) Risikomanagementstrategie .....	777
(2) Risikotragfähigkeitskonzept. ....	777
(3) Interne Kontrollverfahren .....	778
(4) Personelle und technische Ausstattung. ....	778
(5) Notfallkonzept. ....	778
(6) Nachhaltiges Vergütungssystem .....	778
bb) Compliance .....	779
(1) MaRisk BA-Compliance .....	779
(2) MaComp-Compliance .....	780
2. Anforderungen an Unternehmen .....	780
a) Normativer Rahmen und Übertragbarkeit. ....	780
b) Grenzen .....	783
IV. Ausgestaltung des Risikomanagement- und Compliance-Systems im Unternehmensbereich .....	783
1. Finanzproduktbezogenes Risikomanagement und Compliance – Überblick .....	783
2. Die Ausgestaltung der wichtigsten ICRM-Komponenten im Einzelnen .....	785
a) Rechtliche Einzelfallprüfung: Covenant-Tool .....	785
b) Kreditrisiko-Tool .....	786



c) Marktrisiko-Tool .....	787
d) Liquiditätsrisiko-Tool .....	788
3. Delegation des Risikomanagements und Compliance .....	788
V. Haftungsfragen .....	790
1. Verstoß gegen die Pflicht zum Risikomanagement .....	790
2. Verstoß gegen die Pflicht zur Compliance .....	792
3. Einsatz von Künstlicher Intelligenz .....	792
VI. Fazit .....	793

## 22. Kapitel

### **Der Geldwäschebeauftragte – Stellung und Aufgaben**

*(Kaetzler)*

I. Der Geldwäschebeauftragte .....	795
1. Warum eigentlich ein Geldwäschebeauftragter? – Geschichte einer besonderen Funktion .....	796
2. Verpflichtete Unternehmen .....	804
a) Qua Gesetz .....	804
b) Freistellungsmöglichkeit (§ 7 Abs. 2 GwG) .....	806
c) Anordnung der Behörden .....	807
3. Anforderungen an den Geldwäschebeauftragten und Bestellung .....	808
4. Kompetenzen und Stellung im Unternehmen .....	810
5. Aufgaben des Geldwäschebeauftragten .....	814
a) Risikoanalyse .....	815
b) Sicherungsmaßnahmen .....	815
c) Antizipation und Implementierung neuer rechtlicher und verwaltungspraktischer Vorschriften .....	816
d) Kontinuierliche Überwachung von Geschäftsbeziehungen/ „Monitoring“ .....	817
e) Verdachtsfälle und Verdachtsmeldewesen/Unstimmigkeits- meldungen .....	817
f) Berichtswesen, Bericht an Geschäftsleitung und Aufsichtsorgan .....	819
g) Mitarbeiterschulungen .....	819
6. Arbeitsrechtlicher Schutz des Geldwäschebeauftragten und Teilausnahme vom Direktionsrecht des Arbeitgebers .....	820
a) Sonderkündigungsschutz .....	820
b) Benachteiligungsverbot .....	821
c) Ausnahme vom Direktionsrecht .....	822
7. Auslagerung der Funktion .....	822
8. Haftung .....	824
9. Der Geldwäschebeauftragte – gefangen zwischen hoheitlicher und unternehmerischer Tätigkeit? .....	825

23. Kapitel

**Geldwäsche-Compliance in Industrie und Handel**

*(Komma)*

I. Einführung in die Geldwäscheprävention.....	827
1. Begriff und Methoden der Geldwäsche .....	827
2. Die Geldwäschebekämpfung .....	829
a) Geldwäschebekämpfung auf internationaler Ebene: FATF...	829
b) Geldwäschebekämpfung in der deutschen Gesetzgebung ....	830
3. Geldwäscherisiken für Industrie- und Handelsunternehmen ....	832
II. Industrie- und Handelsunternehmen im GwG:	
Der Begriff des Güterhändlers.....	834
III. Die Pflichten der Güterhändler im GwG.....	835
1. Die privilegierte Verpflichtetenstellung von Güterhändlern.....	836
a) Praktische Umsetzung des Bargeldausschlusses .....	836
b) Konsequenzen bei Einführung einer Bargeldbeschränkung ..	838
2. Risikomanagement .....	839
a) Risikoanalyse .....	839
b) Interne Sicherungsmaßnahmen.....	841
aa) Richtlinie zur Prävention von Geldwäsche .....	842
bb) Überprüfung von Geschäftspartnern.....	842
cc) Überwachung von Zahlungseingängen .....	842
c) Gruppenweite Pflichten .....	843
3. Kundensorgfaltspflichten.....	844
a) Auslösetatbestände der Sorgfaltspflichten für Güterhändler..	844
b) Ausgewählte Aspekte der allgemeinen Sorgfaltspflichten ...	846
c) Ausgewählte Aspekte der vereinfachten und verstärkten Sorgfaltspflichten.....	847
4. Pflicht zur Abgabe von Verdachtsmeldungen .....	848
a) Verdachtsfall und typische Verdachtsmomente .....	848
b) Folgen einer Verdachtsmeldung .....	850
aa) Strafbefreiende Wirkung.....	850
bb) Transaktionssperrfrist § 46 GwG.....	851
cc) Verbot der Informationsweitergabe (Tipping Off-Verbot)	851
IV. Fazit .....	852

24. Kapitel

**Sanktions-Compliance als Teil eines effektiven  
Compliance-Management-Systems**

*(Salathé/Moussaoui)*

I. Einleitung .....	855
1. Terminologien und Begriffsverständnis .....	856

2. Sanktionen: Historie, Gründe und Ziele .....	857
<b>II. Rechtsrahmen .....</b>	<b>858</b>
1. UN-Sanktionen.....	858
2. EU-Sanktionen .....	859
a) Anwendungsbereich.....	859
b) Grundlage der EU-Sanktionen.....	861
c) Auslegung der EU-Sanktionen.....	862
3. Aufbau der EU-Sanktionen .....	863
a) Listenprinzip .....	863
b) Finanzsanktionen .....	864
aa) Begriffsdefinitionen .....	864
(1) Gelder .....	865
(2) Wirtschaftliche Ressourcen.....	865
(3) Einfrieren von Geldern und wirtschaftlichen Ressourcen .....	866
(4) Eigentum und Besitz.....	867
(5) Halten und Kontrollieren .....	867
bb) Bereitstellungsverbot .....	869
(1) Bereitstellung.....	869
(2) Mittelbare Bereitstellung.....	870
cc) Einfriergebot .....	871
dd) Ausnahmen.....	872
4. Deutschland.....	873
a) Außenwirtschaftsgesetz und Außenwirtschaftsverordnung...	873
b) Sanktionsdurchsetzungsgesetze.....	874
5. Ausblick: Deutschland und EU.....	876
6. US-Sanktionen .....	877
a) Grundlagen .....	877
b) Anwendungsbereich.....	878
aa) Primärsanktionen.....	878
bb) Sekundär-Sanktionen .....	879
c) Funktionsweise der US-Sanktionen .....	880
7. Anti-Boycott-Regelungen .....	881
a) EU-Blocking-Verordnung.....	881
aa) Hintergrund der EU-Blocking-Verordnung .....	881
bb) Regelungen der EU-Blocking-Verordnung .....	882
b) § 7 AWV.....	883
8. Weitere Sanktionen anderer Staaten und Organisationen .....	884
<b>III. Konsequenzen und Haftung .....</b>	<b>885</b>
1. Straf- und ordnungswidrigkeitsrechtliche Folgen .....	885
a) § 17 AWG.....	885
b) § 18 AWG.....	885
c) § 19 AWG.....	886

d) Vermeidung von Verstößen .....	887
2. Zivilrechtliche Folgen .....	887
3. Schadensersatz .....	889
4. Sonstige Folgen .....	889
IV. Maßnahmen zur Umsetzung eines Sanktions-Compliance- Management-Systems .....	890
1. Risikobewertung .....	891
2. Know Your Business Partner/Know Your Customer/ Risikoanalyse .....	892
a) Phase 1: Informationsbeschaffung .....	893
b) Phase 2: Überprüfung .....	894
c) Phase 3: Risikoeinschätzung .....	895
d) Phase 4: Entscheidung .....	895
3. Interne Meldeprozesse und Ablauforganisation .....	895
4. Tone from the Top und Guidance .....	896
5. Mitarbeiterzuverlässigkeit .....	897
6. Schulungen .....	898
7. Überprüfung .....	898
8. Rechtliche Unterstützung .....	899
9. Einsatz von IT-Hilfen/Technik .....	899
10. Dokumentation und Aufbewahrung .....	899
V. Checkliste .....	900

25. Kapitel

**Exportkontrolle und Compliance**

*(v. Bodungen)*

I. Einleitung .....	903
II. Rechtsgrundlagen der Exportkontrolle in Deutschland .....	904
1. Supranationale Vorgaben .....	904
2. Nationale Vorgaben .....	906
3. Relevanz ausländischen Exportkontrollrechts .....	906
a) Allgemeines .....	906
b) Insbesondere: US-Re-Exportkontrolle .....	906
III. Exportkontrollrechtliche Genehmigungspflichten .....	908
1. Allgemeines .....	908
2. Genehmigungspflichten bei Ausfuhren in Länder außerhalb der EU .....	908
a) Gelistete Güter .....	908
b) Nicht gelistete Güter .....	909
3. Genehmigungspflichten bei Verbringungen .....	910
a) Verbringungen bei Endverbleib in der EU .....	910

b) Verbringungen mit anschließender Ausfuhr .....	910
4. Sonstige Genehmigungspflichten .....	911
a) Handels- und Vermittlungsgeschäfte .....	911
b) Technische Unterstützung .....	911
IV. Exportkontrollrechtliches Genehmigungsverfahren .....	912
1. Zuständigkeit des BAFA .....	912
2. Ablauf des Genehmigungsverfahrens .....	913
3. Genehmigungstypen .....	914
4. Sanktionen bei exportkontrollrechtlichen Verstößen .....	915
V. Exportkontrollrechtliche Compliance-Strukturen .....	916
1. Allgemeines .....	916
2. Der Ausfuhrverantwortliche .....	918
3. Modell eines innerbetrieblichen Exportkontrollsystems .....	919
a) Überblick über die relevanten Strukturelemente .....	920
b) Umsetzung im Einzelfall .....	922
VI. Zusammenfassung und Ausblick .....	924

## 26. Kapitel

### Compliance in M&A-Transaktionen

(Ullrich)

I. Einleitung .....	927
II. Prozessuale M&A-Compliance – Einhaltung von Rechtsvorschriften im M&A-Verfahren .....	928
1. Strukturierung der Transaktion .....	928
a) Auktions- und Einzelbieterverfahren .....	928
b) Transaktionsgegenstand .....	929
2. Offenlegung von Informationen .....	929
a) Offenlegungs- und Aufklärungspflichten des Veräußerers .....	929
b) Rechtliche Grenzen der Offenlegung von Informationen .....	931
aa) Gesellschaftsrechtliche Zulässigkeit der Offenlegung von Informationen gegenüber Dritten .....	931
bb) Vertraulichkeitsbestimmungen in Verträgen mit Dritten ..	933
cc) Datenschutzrechtliche Anforderungen für die Offenlegung von personenbezogenen Daten .....	934
3. Kartellrechtliche M&A-Compliance – Vollzugsverbot, Marktmachtmissbrauch und Informationsaustausch .....	936
a) Anmeldepflicht und Vollzugsverbot .....	936
b) Informationsaustausch .....	939
4. Kapitalmarktrechtliche M&A-Compliance .....	942
a) Informationsweitergabe im Rahmen der Due Diligence .....	942
b) Ad-hoc-Pflicht .....	943

c) Übernahmerechtliche M&A-Compliance.....	944
5. Pflicht zur Durchführung einer rechtlichen Due Diligence .....	945
a) Regelfall.....	945
b) Besonders gelagerte Fälle.....	946
c) Nachgelagerte Due Diligence (Post-Closing Due Diligence) .	948
6. (Abbruch der) Vertragsverhandlungen .....	948
7. Zustimmungserfordernisse .....	950
a) Zustimmung von Aufsichtsgremien und/oder der Gesellschafter .....	950
b) Zustimmung von Ehegatten oder Lebenspartnern.....	954
8. Vereinbarung von Wettbewerbsverboten im Unternehmens- kaufvertrag .....	956
III. Materielle M&A-Compliance – Prüfung von/Umgang mit Compliance in der Zielgesellschaft .....	957
1. Due Diligence .....	957
a) Erfordernis einer Compliance-Due Diligence .....	957
aa) Einführung unter besonderer Beachtung von ESG/CSR .	957
bb) Erfordernis der Durchführung einer Compliance-Due Diligence .....	959
cc) (Eigen-)Interesse der Geschäftsleitung (Business Judgement Rule).....	961
dd) Normative Kraft des Faktischen.....	962
b) Vorgehensweise: Abgestufte, risikobasierte Compliance-Due Diligence .....	962
aa) Rechtlicher Rahmen.....	962
bb) Ermittlung des Risikoprofils der Zielgesellschaft .....	963
cc) Risikobewertung und Dokumentation .....	964
dd) Eigentliche Due Diligence .....	964
c) Due Diligence nach Vollzug .....	964
2. Umgang mit bekannten/bekanntgewordenen Compliance- Verstößen/-Risiken .....	965
a) Risikobewertung .....	965
b) Umgang mit bekannten/entdeckten Compliance-Risiken ....	966
IV. Zusammenfassung .....	969

## 27. Kapitel

### Kartellrechts-Compliance

(Seeliger/Mross/Seydel)

I. Überblick über die Kartellrechts-Risiken .....	971
1. Einleitung .....	971
2. Kartellrechts-Risikokategorien.....	973
a) Das Verbot wettbewerbsbeschränkender Vereinbarungen: Absprachen mit anderen Unternehmen .....	974

aa) Vereinbarung, abgestimmtes Verhalten oder Beschluss ..	974
bb) Bezweckte oder bewirkte Wettbewerbsbeschränkung ....	975
cc) Sehr hohe Risiken .....	976
(1) „Hardcore-Kartelle“ .....	976
(2) Ausschreibungen .....	977
(3) Informationsaustausch .....	978
(4) Verbandsarbeit .....	980
(5) Preisbindungen und Preisempfehlungen .....	981
(6) Marktaufteilungen beim Vertrieb .....	982
(7) Internet-Behinderungen .....	983
(8) Boykott .....	986
(9) Personalbereich .....	986
dd) Weniger hohe Risiken .....	987
(1) Horizontale Kooperationen .....	987
(2) Vertriebsbeschränkungen .....	991
(3) Wettbewerbsverbote (Markenzwang); Alleinbezugsverpflichtungen .....	993
b) Machtmissbrauch (einseitige Handlungen) .....	994
aa) Allgemeine Voraussetzungen .....	994
(1) Marktbeherrschende Stellung .....	995
(2) Missbräuchliche Ausnutzung .....	996
bb) Sehr hohe Risiken .....	996
(1) Behinderung/Ausgrenzung von Wettbewerbern .....	996
(2) Kundenbindung, Treuerabatte .....	997
(3) Squeeze-out von Wettbewerbern, Kosten-Preis- Schere .....	997
(4) Kopplung von Angeboten .....	997
cc) Weniger hohe Risiken .....	998
(1) Ausbeutungsmissbrauch, Kundenpreis- differenzierung .....	998
(2) Niedrigpreisstrategien .....	998
(3) Lieferverweigerung; wesentliche Einrichtungen („Essential Facilities“) .....	999
(4) Ausschließlichkeitsbindungen .....	999
(5) Diskriminierung abhängiger Unternehmen .....	999
(6) Behinderung von kleineren Wettbewerbern; Verkauf unter Einstandspreis .....	1000
3. Haftungssubjekte (Wer haftet für wen?) .....	1000
a) Unternehmenshaftung .....	1000
b) Persönliche Haftung .....	1001
c) Haftung im Konzern („Wirtschaftliche Einheit“) .....	1002
d) Haftung bei Gemeinschaftsunternehmen .....	1003
e) Haftung für Beauftragte .....	1003
f) Haftung bei Rechtsnachfolge .....	1004

4. Art und Umfang der Haftung .....	1005
a) Strafrechtliche Sanktionen .....	1005
b) Bußgelder .....	1006
aa) EU-Recht .....	1006
bb) Deutsches Recht .....	1007
c) Schadensersatz .....	1009
aa) Individualansprüche .....	1009
bb) Kollektiver Rechtsschutz .....	1011
cc) Schadensausgleich im Innenverhältnis .....	1012
d) Sonstige Nachteile .....	1012
II. Management der Kartellrechtsrisiken in der Praxis .....	1013
1. Risikoanalyse: Identifizierung und Bewertung .....	1015
a) Kartellrechtliches Risikoprofil .....	1015
b) Geschäftstätigkeit und Geschäftsbeziehungen .....	1015
c) Risikokategorisierung und Risikobewertung .....	1016
d) Einführung eines Top-down-Ansatzes .....	1017
2. Präventive Maßnahmen .....	1017
a) Richt- und Leitlinien zum Kartellrecht .....	1018
b) Schulungen (Präsenzs Schulungen und Webinars/E-Learning) ..	1021
3. Maßnahmen zur Kontrolle/Aufdeckung .....	1023
III. Behördliche Untersuchungen .....	1025
1. Durchsuchungen der EU-Kommission .....	1026
a) Zuständigkeit .....	1026
b) Befugnisse .....	1027
c) Elektronische Durchsuchung .....	1028
d) Typischer Ablauf .....	1029
2. Durchsuchungen des Bundeskartellamts .....	1030
a) Zuständigkeit .....	1030
b) Befugnisse .....	1031
c) Elektronische Durchsuchung .....	1033
d) Typischer Ablauf .....	1034
3. Verhaltensregeln für die Unternehmen .....	1034
a) Vor der Durchsuchung .....	1034
b) Während der Durchsuchung .....	1035
c) Nach der Durchsuchung .....	1037

## 28. Kapitel

### **Compliance-Anforderungen im Wettbewerb um öffentliche Aufträge** (Scherer)

I. Einleitung .....	1039
II. Anforderungen an Unternehmen in Vergabeverfahren .....	1040



III. Ausschlussgründe .....	1042
1. Zwingende Ausschlussgründe .....	1042
a) Straftatbestände .....	1042
b) Steuer- und Abgabentatbestände .....	1043
2. Fakultative Ausschlussgründe .....	1044
a) Verstoß gegen umwelt-, sozial- oder arbeitsrechtliche Verpflichtungen .....	1044
b) Insolvenz und Liquidation .....	1045
c) Schwere Verfehlung im Rahmen beruflicher Tätigkeit .....	1045
d) Wettbewerbsbeschränkende Vereinbarungen oder abgestimmte Verhaltensweisen .....	1046
e) Interessenkonflikt .....	1047
f) Vorbefassung .....	1047
g) Mangelhafte Leistung bei Ausführung früherer Aufträge ....	1048
h) Schwerwiegende Täuschung bei Eignungsprüfung .....	1048
i) Unzulässige Einflussnahme .....	1049
IV. Wettbewerbsregister .....	1050
1. Einrichtung des Wettbewerbsregisters .....	1050
2. Eintragung von Rechtsverstößen .....	1050
3. Einbindung in das Vergabeverfahren .....	1051
4. Löschung von Eintragungen .....	1052
5. Rechtsbehelfe .....	1053
V. Selbstreinigung .....	1053
1. Selbstreinigung im Vergabeverfahren .....	1053
a) Prüfung durch Vergabestelle .....	1053
b) Prüfung durch Wettbewerbsregister .....	1054
2. Kriterien der Selbstreinigung .....	1054
a) Ausgleich des Schadens .....	1054
b) Zusammenarbeit zur Aufklärung .....	1055
c) Technische, organisatorische und personelle Maßnahmen ....	1056
VI. Ausschlussfristen .....	1058
1. Fristenregelung bei zwingenden Ausschlussgründen .....	1058
2. Fristenregelung bei fakultativen Ausschlussgründen .....	1058
3. Ermessensausübung .....	1059

29. Kapitel  
**Tax Compliance**  
(Schwartz)

I. Einleitung .....	1061
II. Steuerliche Pflichten .....	1063

1. Allgemeine steuerliche Pflichten .....	1063
2. Spezifische materiell-rechtliche Problemschwerpunkte .....	1068
a) Lohnsteuer und Sozialabgaben .....	1068
b) Umsatzsteuer.....	1069
c) Verdeckte Gewinnausschüttungen .....	1070
d) Anzeigepflicht nach § 153 AO .....	1071
e) Tochtergesellschaften und Betriebstätten im Ausland .....	1074
f) Internationale Verrechnungspreise.....	1075
g) Versagung des Betriebsausgabenabzugs nach § 160 AO .....	1075
h) Betriebsausgabenabzugsverbot nach § 4 Abs. 5 Satz 1 Nr. 10 EStG .....	1076
III. Risiken mangelnder Tax Compliance .....	1078
1. Steuerliche Haftungsrisiken .....	1078
2. Steuerstrafrechtliche und steuerordnungswidrigkeitenrechtliche Risiken.....	1080
a) Sanktionen gegen Organe und Mitarbeiter .....	1080
aa) Steuerhinterziehung und leichtfertige Steuerverkürzung (§§ 370, 378 AO) .....	1080
(1) Täter .....	1080
(2) Objektiver Tatbestand .....	1081
(3) Subjektiver Tatbestand .....	1085
(4) Strafe.....	1086
bb) Verletzung der Aufsichtspflicht (§ 130 OWiG).....	1087
b) Sanktionen gegen das Unternehmen .....	1088
aa) Verbandsgeldbuße (§ 30 OWiG) .....	1088
bb) Einziehung (§ 29a OWiG).....	1090
IV. Tax Compliance-System.....	1091
1. Risikoanalyse .....	1091
2. Ausgestaltung eines Tax Compliance-Systems.....	1092
a) Zuständigkeit für Tax Compliance.....	1092
b) Zuständigkeit und Verantwortlichkeit bzgl. der steuerlichen Pflichten.....	1092
c) Berichtswege/Berichtspflichten .....	1093
d) Prozessbeschreibung Deklarationswesen .....	1095
e) Kontroll- und Überwachungsmaßnahmen .....	1095
f) Umgang mit Betriebsprüfungen .....	1096
g) Schulungen .....	1098
h) Dokumentation.....	1098
3. Prüfungserleichterungen nach Art. 97 § 38 EGAO.....	1099
a) Tatbestandsvoraussetzungen .....	1099
b) Rechtsfolgen .....	1101
V. Zertifizierung des Tax Compliance-Systems durch Dritte .....	1102

VI. Berichtigung von Steuererklärungen .....	1104
1. Korrekturvorschrift .....	1104
2. Selbstanzeige im Unternehmen (§§ 371, 378 Abs. 3 AO) .....	1105
a) Person des Anzeigerstatters .....	1105
b) Positive Wirksamkeitsvoraussetzungen des § 371 AO .....	1106
c) Negative Wirksamkeitsvoraussetzungen des § 371 AO (Sperrgründe) .....	1108
d) Absehen von Verfolgung nach § 398a AO .....	1111
e) Bußgeldbefreiende Selbstanzeige nach § 378 Abs. 3 AO .....	1112
VII. Fazit .....	1112
Literaturverzeichnis .....	1113
Sachregister .....	1157