

Inhalt

Vorwort	V
Autorenverzeichnis	VII
Abkürzungsverzeichnis	XLIII

Teil 1 Kernelemente und Handlungsstrategien

1. Kapitel Compliance-Management – Grundlagen, Zusammenhänge und Strategien (Schulz)	1
I. Grundlagen und Zusammenhänge	1
1. Compliance-Management als Führungs- und Organisationsaufgabe	1
a) Verbindung von Compliance und Integritäts- management	2
b) Zunahme von Rechts- und Compliance-Risiken	5
c) Corporate Governance und CSR als dynamische Bezugsrahmen	7
d) Relevanz für alle Unternehmen	9
e) Nachteile von Regelverletzungen („Non-Compliance“).	10
f) Besondere Merkmale von Compliance-Risiken.	11
g) Parallelen und Unterschiede zum allgemeinen Risikomanagement	12
h) Compliance-Pflicht als verbandsübergreifendes Prinzip	14
i) Grundfragen verantwortungsvoller Unternehmens- führung	15
2. Ziele und Vorteile von Compliance-Management	17
a) Prävention, Aufdeckung und Sanktionierung von Regelverletzungen	17
b) Förderung von Regeltreue und Integrität („Compliance-Kultur“)	17
c) Schutz von Unternehmen, Geschäftsleitern und Mitarbeitern	18
d) Sicherung der Reputation des Unternehmens	18
e) Wahrung rechtlicher Gestaltungsmöglichkeiten.	19
f) Vorteile im Marketing und Imagegewinn bei Bezugsgruppen	20
	XV

Inhaltsverzeichnis

	g) Verteidigungsmöglichkeit im Fall von „Non-Compliance“	21
	h) Verbesserung von Strukturen und Prozessen	21
II.	Vorgaben und Orientierungshilfen	22
	1. Branchenspezifische Sonderregeln als Erkenntnisquelle	23
	2. Compliance-Pflicht als Ausprägung der Leitungsverantwortung	24
	3. Notwendigkeit eines Compliance-Risikomanagements.	25
	4. Anforderungen an Aufsichts- und Überwachungsmaßnahmen	26
	5. Vorgaben der Unternehmensorganisations- und Garantepflichten	27
	6. Einfluss von Vorschriften anderer Rechtsordnungen	28
	7. Bedeutung von Compliance-Standards (Beispiel IDW PS 980)	29
III.	Kernelemente und Erfolgskriterien	30
	1. Handlungsspielraum bei der Ausgestaltung des Compliance-Managements	30
	2. Konzeption einer Compliance-Strategie	31
	a) Wahl eines unternehmensspezifischen Organisationsmodells.	32
	b) Verankerung einer Integritäts- und Compliance-Kultur	33
	aa) Authentisches Bekenntnis zu Regeltreue und Integrität durch die Geschäftsleitung	34
	bb) Aufnahme von Compliance in das Unternehmensleitbild („Mission Statement“)	35
	cc) Formulierung und Kommunikation von Leitwerten („Code of Conduct“)	35
	dd) Effektive Vermittlung von Compliance und Integrität als Personalführungsaufgabe.	36
	c) Entwicklung einer Compliance-Risikostrategie.	37
	aa) Systematische Identifikation von Compliance-Risiken	38
	bb) Analyse und Bewertung	39
	cc) Entwicklung von Risikosteuerungsmaßnahmen	39
	dd) Berichterstattung zu Compliance-Risiken	40
	ee) Regelmäßige Compliance-Audits.	40
	d) Klärung von Zuständigkeiten und Delegationsmöglichkeiten	41
	e) Schlüsselrolle der Compliance Officer	42

f)	Integration von Compliance in die Geschäftsprozesse . . .	43
g)	Koordination weiterer Unternehmensfunktionen	44
h)	Initiierung bedarfsgerechter Schulungen und Fortbildungsangebote	45
i)	Einrichtung von Kontrollen und Feedback-Prozessen. . .	45
j)	Aufklärung von Verstößen	46
k)	Konsequente Sanktionierung von regelwidrigem und unethischem Verhalten.	46
l)	Sicherstellung regelmäßiger Aktualisierung	47
IV.	Leitlinien und Empfehlungen	47
2. Kapitel Einführung eines „Code of Conduct“		
	<i>(Benkert)</i>	51
I.	Einleitung	51
II.	Ausgestaltung	52
	1. Erscheinungsformen	52
	2. Typische Regelungen	55
III.	Einführung eines „Code of Conduct“	57
	1. Individualvertragliche Umsetzung	58
	a) Weisungsrecht des Arbeitgebers.	58
	b) Vertragliche Vereinbarung.	60
	c) Änderungskündigung	62
	2. Betriebsvereinbarung	62
IV.	Mitbestimmungsrecht des Betriebsrats	65
3. Kapitel Whistleblowing-Systeme – Aufbau und Management		
	<i>(Möhlenbeck)</i>	69
I.	Einleitung	69
	1. Begriffsbestimmung	70
	2. Gründe für die Einführung eines Whistleblowing-Systems	71
	3. Rechtliche Rahmenbedingungen	72
	a) Internationale Anforderungen	72
	aa) Sarbanes Oxley Act (SOX)	72
	bb) Dodd-Frank Act	73
	cc) UK Bribery Act (UKBA).	74
	dd) OECD-Übereinkommen vom 17.12.1997.	74
	b) Rechtslage in Deutschland.	75
	aa) Gesellschaftsrechtliche Vorgaben	75
	bb) Ordnungswidrigkeitenrechtliche Vorgaben.	75

Inhaltsverzeichnis

	cc) Vorgaben des Deutschen Corporate Governance Kodex	76
	dd) Vorgaben aus der Rechtsprechung	76
II.	Überblick über die mögliche Ausgestaltung von Hinweismanagementsystemen	77
	1. Externes Whistleblowing	77
	2. Internes Whistleblowing	77
	3. Mögliche Begrenzungen (Hinweisgeber, Empfänger, Themen)	78
III.	Aufbau/Einführung eines Hinweismanagementsystems	78
	1. Rechtliche Anforderungen	78
	a) Rechtslage in Deutschland.	78
	b) Vorgaben auf europäischer Ebene	79
	c) Regelungen in den USA und Großbritannien	81
	aa) USA	81
	bb) Großbritannien	81
	2. Datenschutzrechtliche Anforderungen	81
	a) Anforderungen des Bundesdatenschutzgesetzes	82
	b) Empfehlungen der Ad-hoc-Arbeitsgruppe „Beschäftigtendatenschutz“ des Düsseldorfer Kreises	82
	3. Entscheidungen hinsichtlich der konkreten Ausgestaltung	83
	a) Organisation	83
	b) Ausgestaltungsmöglichkeiten	84
	aa) Kreis der Hinweisgeber	84
	bb) Eingangskanäle	85
	cc) Arten der meldbaren Verstöße	87
	dd) Regelungen zur Einführung eines Hinweismanagementsystems	87
	4. Kommunikation	88
IV.	Die praktische Arbeit mit einem Whistleblowing-System	89
	1. Schutz des Hinweisgebers vor Nachteilen	89
	2. Schutz des Betroffenen	90
	3. Datenschutzkonformer Umgang mit eingegangenen Hinweisen	90
V.	Fazit	91
	4. Kapitel Kommunikationsmanagement und Schulungen (Hastenrath)	93
I.	Einleitung	93
II.	Grundzüge zur Kommunikation in der Unternehmenspraxis.	94

1.	Relevanz der Kommunikation im Unternehmen und bei Compliance	94
2.	Kommunikationsmodelle	96
a)	Modell zu Konfliktarten als Grundlage für die Kommunikation	96
b)	Praxisrelevantes Beispiel	99
III.	Ausgewählte Instrumente der Compliance-Kommunikation . .	102
1.	Tone-From-The-Top	102
2.	Persönlicher Kontakt mit dem Compliance Officer	102
3.	Zusammenarbeit des Compliance Officers mit Schlüsselfunktionen im Unternehmen	103
4.	Schriftliche Informationen an die Mitarbeiter	103
5.	Compliance im firmeneigenen Intranet	104
IV.	Schulungen	105
1.	Persönliche Schulungen durch die Compliance-Funktion . .	105
2.	Schulungen mit klassischem E-Learning	106
3.	Schulungen mit Webinaren	107
4.	Unterstützung dezentraler Compliance-Funktionen: das Schulungshandbuch	119
V.	Die „Top 5 Stolpersteine“ in der Compliance-Kommunikation und Lösungsvorschläge	121
1.	Fehlende, verspätete oder missverständliche Information . .	121
a)	Problemstellung	121
b)	Lösungsvorschlag	122
2.	Mangelnde Authentizität („Nicht gelebte Hochglanzaussagen“)	123
a)	Problemstellung	123
b)	Lösungsvorschlag	123
3.	Fehler im Kommunikationsmanagement: Budget- und Ressourcenmangel	124
a)	Problemstellung	124
aa)	Unzureichende Übersetzung eines Code of Conduct (CoC)	125
bb)	Unzureichendes Schulungsbudget	126
b)	Lösungsvorschlag	127
4.	Probleme mit der Technik	128
a)	Problemstellung	128
b)	Lösungsvorschlag	128

Inhaltsverzeichnis

5.	Fehler im Kommunikationsmanagement von Compliance aufgrund von Kulturunterschieden	130
a)	Problemstellung	130
b)	Lösungsvorschlag	131
VI.	Fazit zur Compliance-Kommunikation	132
5. Kapitel Integration des Compliance-Managements in den betrieblichen Steuerungsprozess – Beispiel Immobilienmanagement		
	<i>(Muth)</i>	135
I.	Einleitung	135
II.	Compliance Management in der Prozess-Perspektive („Prozessmodell Compliance“)	136
1.	Der Prozess für Aufbau und Implementierung eines CMS	137
2.	Besondere Compliance-Prozesse	139
3.	Compliance in Fachprozessen – Verankerung in branchenspezifischen Abläufen	140
4.	Der Steuerungsprozess Compliance	142
5.	Die Integration der Prozesse	143
a)	Prozesslandkarte Compliance	143
b)	Das Prozessmodell Compliance – verdichtet	143
c)	Die Zusammenführung des CMS-Prozesses mit dem Prozessmodell des Unternehmens	144
III.	Die Integration von Compliance am Beispiel eines Geschäftsmodelles „Immobilienmanagement“.	145
IV.	Steigerung der Compliance-Reife des Unternehmens durch messbare Zielvereinbarungen	147
1.	Verankerung von risiko-zentrierten Compliance-Kontrollen in Arbeitsabläufen	147
2.	Messen der ordnungsgemäßen Anwendung der implementierten Compliance-Absicherungen	151
3.	Festlegen messbarer Compliance-Ziele als Maßstab für die Compliance-Reife des Unternehmens.	152
V.	Fazit	154
6. Kapitel Auswirkungen des ISO-Standards 19600 auf die Prüfung von Compliance-Management-Systemen nach IDW PS 980		
	<i>(Withus)</i>	157
I.	Einleitung	157
II.	Zielsetzung und Zielgruppe	158
1.	Ausgangslage	158
2.	Zielsetzung des IDW PS 980	158

	3. Zielsetzung des ISO 19600:2014	159
	4. Vergleich	159
III.	Unterschiedliche Regelungstiefe zur Ausgestaltung des CMS . .	159
	1. CMS-bezogene Regelungsinhalte des IDW PS 980	159
	2. Regelungsinhalte des ISO 19600:2014	160
IV.	ISO 19600 als geeignetes, angemessenes Rahmenkonzept für ein CMS.	163
	1. Anforderungen des IDW PS 980 an ein Rahmenkonzept . .	163
	2. Vergleich ISO 19600 Guidelines mit IDW PS 980-Grundelementen	165
V.	Zwischenergebnis	167
VI.	Argumente für eine Ausrichtung des CMS nach ISO 19600. .	167
	1. Basis für Ermessensentscheidung und Compliance-Richtlinie	167
	2. Beurteilung der angemessenen Einrichtung eines wirksamen CMS	169
VII.	Zusammenfassung	171

Teil 2 Übergreifende Herausforderungen

7. Kapitel Risikomanagement – Einführung und methodischer Überblick

	(J. Becker)	173
I.	Einleitung	173
II.	Grundzüge des unternehmerischen Risikomanagements. . . .	174
	1. Das Risikomanagement als unternehmerisches Steuerungsinstrument	174
	2. Ansätze zur Risikosystematisierung	178
	a) Finanzwirtschaftliche Risiken	178
	aa) Marktpreisrisiken	178
	bb) Ausfallrisiken	179
	cc) Liquiditätsrisiken	179
	b) Leistungswirtschaftliche Risiken: Die Leistungserstellung eines Unternehmens unterliegt ebenfalls zahlreichen Risiken.	180
	aa) Operative Risiken	180
	bb) Absatzrisiken	181
	3. Der Risikomanagementprozess	181
	a) „Bottom up-Verfahren“	183

Inhaltsverzeichnis

	b) „Top down-Verfahren“	183	
III.	Risikoidentifikation	185	
	1. Verfahren zur Erstellung eines Risikokatalogs	185	
	2. Prognose- und Früherkennungssysteme	187	
IV.	Risikoquantifizierung	189	
	1. Beispiel Bottom up-Verfahren	190	
	2. Top down-Verfahren	192	
V.	Herausforderungen des Risikomanagements	194	
VI.	Fazit Risikomanagement	196	
8. Kapitel Governance, Risk und Compliance Management – Zusammenhänge und Abhängigkeiten			
<i>(Bartuschka)</i>			197
I.	Einleitung – Die Notwendigkeit der Einrichtung von Instrumenten zur Überwachung von Unternehmen	197	
II.	Das System der Unternehmensüberwachung	200	
	1. Überblick über das Gesamtsystem	200	
	2. Externe Komponenten der Unternehmensüberwachung	200	
	3. Interne Komponenten der Unternehmensüberwachung	202	
III.	Die Verknüpfung der einzelnen Elemente der Unternehmensüberwachung	203	
	1. Der GRC-Ansatz	203	
	2. Das interne Kontrollsystem und die anderen Elemente der Überwachung des Unternehmens	204	
	3. Compliance- und Risikomanagement	206	
	4. Risikomanagement und Controlling	206	
	5. Interne Revision, Compliance und Risikomanagement	207	
	6. Fazit	208	
IV.	Grundkonzept für die Ausgestaltung eines integrierten Systems der Überwachung für mittelständisch geprägte Unternehmen	208	
	1. Bestimmung der Zielgruppe der Unternehmen	208	
	2. Zielstellung für die Einführung eines integrierten Systems der Überwachung	209	
	3. Vorgehensweise	209	
	a) Risikoanalyse	209	
	b) Analyse bestehender Strukturen	211	
	c) Ermittlung des Anpassungsbedarfs	211	
	d) Umsetzung	211	
	4. Fazit	213	

9. Kapitel Risikomanagement und Compliance bei der Nutzung von Finanz- und Kapitalmarktprodukten	
<i>(Kessler)</i>	215
I. Einleitung	215
II. Finanz- und Kapitalmarktprodukte; Risiken	216
1. „Einfache“ Produkte	216
2. „Komplexe“ Produkte	217
a) Überblick	217
b) Risiken im Einzelnen	220
III. Rechtliche Anforderungen an das Risikomanagement- und Compliance-System	222
1. Anforderungen an Finanzinstitute	222
a) Aufsichtsrechtliche Anforderungen	222
b) „Best Practice“ und praktische Ausgestaltung	224
aa) Risikomanagement	224
(1) Risikomanagementstrategie	225
(2) Risikotragfähigkeitskonzept	225
(3) Interne Kontrollverfahren	226
(4) Personelle und technische Ausstattung	226
(5) Notfallkonzept	226
(6) Nachhaltiges Vergütungssystem	226
bb) Compliance	227
(1) MaRisk BA-Compliance	227
(2) MaComp-Compliance	228
2. Anforderungen an Unternehmen	229
a) Normativer Rahmen und Übertragbarkeit	229
b) Grenzen	231
IV. Ausgestaltung des Risikomanagement- und Compliance-Systems im Unternehmensbereich	231
1. Finanzproduktbezogenes Risikomanagement und Compliance – Überblick	231
2. Die Ausgestaltung der wichtigsten ICRM-Komponenten im Einzelnen	234
a) Rechtliche Einzelfallprüfung: Covenant-Tool	234
b) Kreditrisiko-Tool	235
c) Marktrisiko-Tool	236
d) Liquiditätsrisiko-Tool	237
3. Delegation des Risikomanagements und Compliance	238
V. Haftungsfragen	240
1. Verstoß gegen die Pflicht zum Risikomanagement	240

Inhaltsverzeichnis

2.	Verstoß gegen die Pflicht zur Compliance	241
VI.	Fazit	242
10. Kapitel Die Compliance-Funktion in einem Kreditinstitut		
<i>(Renz/Frankenberger)</i> 243		
I.	Einführung: Was ist Compliance?	243
II.	Welche Compliance-Funktionen gibt es in einem Kreditinstitut?	244
1.	Kapitalmarkt-Compliance	245
2.	Zentrale Stelle/sonstige strafbare Handlungen (inkl. Geldwäscheprävention)	246
3.	MaRisk-Compliance	249
4.	Hinweisgebersystem (Whistleblowing)	251
5.	Datenschutz	252
III.	Inhalt und Aufgabe einer modernen Compliance-Funktion	254
IV.	Das Compliance-Management-System (CMS)	255
V.	Schnittstellen zu anderen Funktionen	258
1.	Fach- und Marktbereiche	259
2.	Rechtsabteilung	259
3.	Risikocontrolling-Funktion	260
4.	Interne Revision	261
VI.	Compliance als Teil des IKS eines Kreditinstituts	262
VII.	Übertragung der Struktur/des Ansatzes auf andere Industriesäulen – und umgekehrt	267
VIII.	Fazit/Ausblick	269
11. Kapitel Compliance als Schnittstellenaufgabe – Überlegungen und Anregungen zur erfolgreichen Zusammenarbeit mit anderen Unternehmensfunktionen		
<i>(Rau)</i> 271		
I.	Einleitung	271
II.	Unternehmensfunktionen und ihre Interaktion im Sinne der Compliance	272
1.	Geschäftsleitung.	273
2.	Aufsichtsrat	277
3.	Rechtsabteilung	279
4.	Personalabteilung	282
5.	Betriebsrat	284

6. Finanzfunktion	286
7. Innenrevision	287
8. Wirtschaftsprüfer	288
9. Unternehmenskommunikation	290
10. Andere.	292
III. Fazit	293
12. Kapitel Compliance im Kontext nachhaltigen Supply Chain-Managements <i>(Schleper/Förstl)</i>	297
I. Einleitung	297
II. Nachhaltiges Lieferantenmanagement	298
1. Lieferantenbewertung	299
2. Lieferantenentwicklung	300
3. Lieferantenauswahl	300
4. Lieferantenmonitoring	301
III. Unterschiede entlang der Supply Chain	302
IV. Konfliktmineralien und Due Diligence – „beyond compliance“	304
V. Praxisrelevanz	306
VI. Fazit	308
13. Kapitel Management Interner Untersuchungen <i>(Wettner/Walter)</i>	309
I. Einleitung	309
II. Entscheidung über die Durchführung Interner Untersuchungen	310
1. Entscheidungsbefugte Stellen	310
2. Pflicht zur Aufklärung konkreter Verdachtsfälle	311
3. Interne Untersuchung oder externe Ermittlung?	312
a) Bereits laufendes behördliches Verfahren	312
b) (Noch) kein behördliches Verfahren	313
III. Vornahme von Eilmaßnahmen	314
1. Einrichtung einer zentralen Koordinierungsstelle	314
2. Maßnahmen der Daten- und Beweissicherung	315
3. Arbeitsrechtliche Maßnahmen	315
4. Beachtung von Informations- und Berichtspflichten	316

Inhaltsverzeichnis

IV.	Planung der internen Untersuchung	317
1.	Grundlagen der Planung	317
a)	Beachtung von Recht- und Verhältnismäßigkeit.	317
b)	Beachtung von Risiken und Folgen der internen Untersuchung	318
2.	Festlegung des Untersuchungsgegenstands	319
3.	Bestimmung des Untersuchungsteams und der Verantwortlichkeiten	320
a)	Auswahl von Mitarbeitern und externen Beratern	320
b)	Festlegung von Verantwortlichkeiten und Berichtswegen	321
4.	Bestimmung und Vorbereitung der Informationsquellen	322
a)	Relevante Informationsquellen	322
aa)	Dokumente	322
bb)	Elektronische Daten und E-Mails	323
cc)	(Ehemalige) Mitarbeiter	323
b)	Notwendige Abstimmung der geplanten Untersuchungsmaßnahmen	324
aa)	Beteiligung von Betriebsrat oder Sprecherausschuss	324
bb)	Abstimmung mit Ermittlungs- und Aufsichtsbehörden	324
c)	Einrichtung eines Datenraums oder eines „Projektportals“	325
5.	Sicherung der Vertraulichkeit	326
a)	Zugriffsmöglichkeiten Dritter	326
aa)	Beschlagnahme durch Ermittlungsbehörden	326
bb)	Herausgabe von Unterlagen an Versicherer.	327
b)	Begrenzung der E-Mail- und sonstigen schriftlichen Kommunikation	328
c)	Kennzeichnung und Aufbewahrung geschützter Kommunikation	328
6.	Erstellen eines Untersuchungsplans.	329
V.	Durchführung der internen Untersuchung	330
1.	Allgemeine Untersuchungsgrundsätze	330
2.	Dokumentation der Untersuchung	331
3.	Erhebung und Auswertung von Dokumenten.	331
4.	Erhebung und Auswertung von elektronischen Daten	332
5.	Befragung von Mitarbeitern	333
6.	Auswertung und Aufarbeitung der Untersuchungs- ergebnisse	335
VI.	Fazit.	337

14. Kapitel CSR und Compliance – Die gesellschaftliche Verantwortung von Unternehmen (<i>Stehr/Struve</i>)	339
I. Einleitung	339
II. Praktische Grundlagen	340
III. Theoretische Grundlagen	343
IV. Ein integratives Konzept von CSR	349
V. CSR und Compliance: Internationales Recht und Soft Law	352
VI. CSR und Compliance in der Strategieentwicklung	355
VII. Die Zukunft von CSR – „CSR 4.0“	357
15. Kapitel CSR-Compliance: Neue Herausforderungen im Reporting (<i>Beisheim</i>)	363
I. Einleitung: Corporate Social Responsibility, Corporate Governance und die (mögliche) Rolle von Compliance	363
II. Neu: Die „CSR-Compliance“	365
1. Zielsetzungen der CSR-Richtlinie und des CSR-Richtlinie- Umsetzungsgesetzes	366
2. Neuausrichtung des Nachhaltigkeitsreportings	367
a) Bestehende Berichtspflichten im deutschen Bilanzrecht	367
b) Sog. „Soft Law-Ansätze“	369
c) Paradigmenwechsel	370
3. Adressaten der neuen Berichtspflichten	371
a) Der Adressatenkreis im Rahmen der nicht-finanziellen Erklärung und der Berichtsvarianten	371
b) Die Verpflichteten der Vorgaben zum Diversitätskonzept	374
4. Berichtsanforderungen im Rahmen der nicht-finanziellen Erklärung und des gesonderten Berichts	375
a) Inhalte, Relevanzmaßstab und Methodik der nicht-finanziellen Erklärung	375
b) Muster: Struktur und Ansätze zur Gestaltung einer nicht-finanziellen Erklärung	380
c) Vorgehensalternativen: Der gesonderte nicht-finanzielle Bericht und die Verwendung von Rahmenwerken.	384
5. Ein Spezifikum: Das Diversitätskonzept	386

Inhaltsverzeichnis

6.	Nichtangaben, unrichtige Angaben und ihre Folgen	386
a)	Der Grundsatz: „Comply or Explain“	387
b)	Ein Sonderfall: Das (vorübergehende) Weglassen nachteiliger Angaben	388
c)	Prüfungen	388
d)	Verstöße, Säumnisse und Sanktionen	390
III.	Fazit und Ausblick	391

Teil 3 Besondere Anwendungsfelder

16. Kapitel Compliance in M&A-Transaktionen (Ullrich)	393
I. Einleitung	393
II. Prozessuale M&A-Compliance – Einhaltung von Rechtsvorschriften im M&A-Verfahren	394
1. Strukturierung der Transaktion	394
2. Offenlegung von Informationen	395
a) Offenlegungs- und Aufklärungspflichten des Veräußerers	395
b) Rechtliche Grenzen der Offenlegung von Informationen	397
aa) Gesellschaftsrechtliche Zulässigkeit der Offenlegung von Informationen gegenüber Dritten	397
bb) Vertraulichkeitsbestimmungen in Verträgen mit Dritten	399
cc) Datenschutzrechtliche Anforderungen für die Offenlegung von personenbezogenen Daten	400
3. Kartellrechtliche M&A-Compliance – Vollzugsverbot und Informationsaustausch	401
a) Anmeldepflicht und Vollzugsverbot	401
b) Informationsaustausch	404
4. Kapitalmarktrechtliche M&A-Compliance	407
a) Informationsweitergabe im Rahmen der Due Diligence	407
b) Ad-hoc-Pflicht	407
c) Übernahmerechtliche M&A-Compliance	409
5. Pflicht zur Durchführung einer rechtlichen Due Diligence a) Regelfall	409
b) Besonders gelagerte Fälle	410
c) In besonders gelagerten Fällen Due Diligence nach Vollzug erforderlich	413
6. (Abbruch der) Vertragsverhandlungen	413

7.	Zustimmungserfordernisse	415
a)	Zustimmung von Aufsichtsgremien und/oder der Gesellschafter	415
b)	Zustimmung von Ehegatten oder Lebenspartnern	417
8.	Vereinbarung von Wettbewerbsverboten im Unternehmens- kaufvertrag	418
III.	Materielle M&A-Compliance – Prüfung von/Umgang mit Compliance in der Zielgesellschaft.	419
1.	Due Diligence	419
a)	Erfordernis einer Compliance-Due Diligence.	419
aa)	Einführung	419
bb)	Erfordernis der Durchführung einer Compliance- Due Diligence.	420
cc)	(Eigen-)Interesse der Geschäftsleitung (Business Judgement Rule)	422
dd)	Normative Kraft des Faktischen	422
b)	Vorgehensweise: Abgestufte, risikobasierte Compliance-Due Diligence	423
aa)	Rechtlicher Rahmen	423
bb)	Ermittlung des Risikoprofils der Zielgesellschaft	424
cc)	Risikobewertung und Dokumentation	425
dd)	Eigentliche Due Diligence	425
c)	Due Diligence nach Vollzug.	425
2.	Umgang mit bekannten/bekanntgewordenen Compliance-Verstößen/-Risiken	426
a)	Risikobewertung.	426
b)	Umgang mit bekannten/entdeckten Compliance-Risiken	427
IV.	Zusammenfassung	430

17. Kapitel Bedeutung und Funktion des Aufsichtsrats beim Compliance-Management (Leupolt)	433
I. Einleitung	433
II. Funktionstrennung, Überwachungsmaßstab und Instrumentarien der Überwachung	433
1. Funktionstrennung und Überwachungsmaßstab	433
2. Instrumentarien der Überwachung	434
a) Prüfungsausschuss.	434
b) Erlangung von Informationen	435

Inhaltsverzeichnis

aa)	Berichterstattung und Befragung des Vorstands . . .	435
bb)	Befragung von Mitarbeitern und Compliance- Verantwortlichen	437
c)	Compliance-Überwachung nach dem Prüfungsstandard IDW EPS 980	438
III.	Die Rolle des Aufsichtsrats bei der Einführung eines Compliance-Management-Systems (CMS)	438
IV.	Die laufende Überwachung des Aufsichtsrats von bestehenden Compliance-Management-Systemen (CMS)	440
1.	Überwachung der laufenden Compliance.	440
2.	Überwachung bei erheblichen Compliance-Verstößen . . .	441
V.	Der Aufsichtsrat bei der Aufklärung von Compliance-Verstößen	442
1.	Überwachung der Aufklärung des Vorstands	442
2.	Eigene Aufklärungszuständigkeit des Aufsichtsrats bei Fehlverstößen des Vorstands	443
VI.	Compliance-Reporting des Aufsichtsrats	444
VII.	Fazit	445
18. Kapitel Compliance Management und Strafrecht		
	<i>(Böttger)</i>	447
I.	Einführung in die Criminal Compliance	447
II.	Strafrechtliche Grundlagen der Compliance-Verpflichtung . .	454
III.	Typische strafrechtliche Compliance-Risiken	458
1.	Korruption	460
a)	Vorteilsgewährung (§ 333 StGB)	464
b)	Bestechung (§ 334 StGB)	471
c)	Bestechung von Mandatsträgern (§ 108e StGB).	473
d)	Bestechung im geschäftlichen Verkehr (§ 299 Abs. 2 StGB)	476
e)	Bestechlichkeit im geschäftlichen Verkehr (§ 299 Abs. 1 StGB)	481
f)	Bestechung im Gesundheitswesen (§ 299b StGB).	481
g)	Auslandskorruption	483
h)	Korruptionsdelikte im weiteren Sinne.	488
2.	Untreue (§ 266 StGB)	490
a)	Generierung von Bestechungsgeld	490
b)	Zahlung von Bestechungsgeld	492

	3. Steuerverkürzung (§§ 370 ff. AO)	493
IV.	Strafrechtliche Risiken der Non-Compliance für die Verantwortlichen des Unternehmens	497
	1. Originäre strafrechtliche Verantwortlichkeit	497
	a) Verantwortlichkeit der Geschäftsleitung	498
	b) Gremienentscheidungen	499
	c) Delegation von Verantwortungsbereichen	500
	d) Verantwortlichkeit des Compliance Officers	502
	e) Aufsichtsrat	504
	2. Innerbetriebliche Anweisungen/Täterschaft kraft Organisationsherrschaft	506
	3. Fahrlässigkeitshaftung (sog. Organisationsverschulden)	507
	4. Verletzung der Aufsichtspflicht in Betrieben und Unternehmen (§ 130 OWiG)	508
V.	Strafrechtliche Risiken der Non-Compliance für das Unternehmen	512
	1. (Unternehmens-)Strafrecht	512
	a) Überblick	512
	b) Verfall und Einziehung	512
	c) Das Unternehmen als Nebenbeteiligter im Strafverfahren	514
	2. Ordnungswidrigkeitenrecht	514
	a) Unternehmensgeldbuße gem. § 30 OWiG	514
	b) Das Unternehmen als Nebenbeteiligter im Verfahren wegen § 30 OWiG	517
	c) Verfall (§ 29a OWiG)	517
VI.	Sonstige Risiken für das Unternehmen und seine Verantwortlichen	518
	1. Blacklisting und Vergabesperren	518
	a) Registereintragungen	518
	aa) Bundeszentralregister	518
	bb) Gewerbezentralregister	518
	cc) Vergabe- bzw. Korruptionsregister	519
	dd) Sonstige Register	521
	b) Vergaberechtliche Konsequenzen	521
	2. Inhabilität (§§ 70 StGB, 6 GmbHG, 76 AktG)	523
	3. Aufsichtsrechtliche Konsequenzen	525
VII.	Strafrechtliche Risiken innerhalb des Compliance-Prozesses („failed compliance“)	526

**19. Kapitel Das Organisationsrisiko der „kriminogenen
Verbandsattitüde“**

<i>(Rack)</i>	531
I. Nützliche Rechtsverstöße zum Vorteil des Unternehmens und zum Nachteil des Mitarbeiters	531
II. Die Theorie der kriminogenen Verbandsattitüde	532
III. Empirische Untersuchungen zur kriminogenen Verbandsattitüde	533
IV. Das Milgram-Experiment zur Gehorsamsbereitschaft gegenüber Autorität	535
V. Konsequenzen für die Organisationspflicht der Organe	536
VI. Die schon vorhandene kriminelle Attitüde im Unternehmen und die Legalitätspflicht zu ihrer Abwehr	537
VII. Die präventive Legalitätspflicht durch Vorstände und Geschäftsführer vor dem Rechtsverstoß	538
VIII. Die unternehmensexterne Aufklärung	539
IX. Die unternehmensinterne Aufklärung	540
X. Die Strafbarkeit von Managern als „Täter hinter dem Täter“ durch Organisationsherrschaft	541
XI. Zwischenergebnis.	542
XII. Kriminelles Mitarbeiterverhalten zum Vorteil des Unternehmens als vorhersehbares Organisationsrisiko.	543
XIII. Die Rechtsgutsferne als Ursache kriminogener Wirkung	545
XIV. Die existentielle Abhängigkeit vom Unternehmen als Ursache kriminogener Wirkungen	546
XV. Der altruistische selbstlose Straftäter als kriminogene Ursache	548
XVI. Die diffuse Verantwortungslosigkeit durch Arbeitsteilung als kriminogene Ursache und die Vermeidung durch die Delegation von Rechtspflichten	548
XVII. Blockierte Informationen als Ursache kriminogener Verbandsattitüden	549
XVIII. Die Auskunftspflicht mit Verwertungsverbot als Konfliktlösung	551
XIX. Fazit	553

20. Kapitel Kartellrechts-Compliance

(Seeliger/Heinen/Mross) 555

I. Überblick über die Kartellrechts-Risiken 555

1. Einführung 555

2. Kartellrechts-Risikokategorien 557

 a) Das Verbot wettbewerbsbeschränkender Vereinbarungen: Absprachen mit anderen Unternehmen 558

 aa) Vereinbarung, abgestimmtes Verhalten oder Beschluss 558

 bb) Bezweckte oder bewirkte Wettbewerbsbeschränkung 559

 cc) Sehr hohe Risiken. 560

 (1) „Hardcore-Kartelle“ 560

 (2) Ausschreibungen 561

 (3) Informationsaustausch 562

 (4) Verbandsarbeit 564

 (5) Preisbindungen und Preisempfehlungen 565

 (6) Marktaufteilungen beim Vertrieb 566

 (7) Internet-Behinderungen 568

 (8) Boykott 570

 dd) Weniger hohe Risiken 570

 (1) Horizontale Kooperationen 570

 (2) Vertriebsbeschränkungen 572

 (3) Wettbewerbsverbote (Markenzwang); Alleinbezugsverpflichtungen 574

 b) Machtmissbrauch (einseitige Handlungen) 575

 aa) Allgemeine Voraussetzungen. 575

 (1) Marktbeherrschende Stellung 575

 (2) Missbräuchliche Ausnutzung 576

 bb) Sehr hohe Risiken. 577

 (1) Behinderung/Ausgrenzung von Wettbewerbern 577

 (2) Kundenbindung, Treuerabatte 577

 (3) Squeeze-out von Wettbewerbern, Kosten-Preis-Schere 578

 (4) Kopplung von Angeboten 578

 cc) Weniger hohe Risiken 578

 (1) Ausbeutungsmissbrauch, Kundenpreisdifferenzierung 578

 (2) Niedrigpreisstrategien 579

Inhaltsverzeichnis

(3) Lieferverweigerung; wesentliche Einrichtungen („essential facilities“)	579
(4) Ausschließlichkeitsbindungen	580
(5) Diskriminierung abhängiger Unternehmen	580
(6) Behinderung von kleineren Wettbewerbern; Verkauf unter Einstandspreis	581
3. Haftungssubjekte (Wer haftet für wen?)	581
a) Unternehmenshaftung	581
b) Persönliche Haftung	582
c) Haftung im Konzern („Wirtschaftliche Einheit“)	583
d) Haftung bei Gemeinschaftsunternehmen	584
e) Haftung für Beauftragte	584
f) Haftung bei Rechtsnachfolge	585
4. Art und Umfang der Haftung	586
a) Strafrechtliche Sanktionen	586
b) Bußgelder	587
aa) EU-Recht	588
bb) Deutsches Recht	589
c) Schadensersatz	590
aa) Individualansprüche	590
bb) Kollektiver Rechtsschutz	592
cc) Preisschirmeffekte	592
dd) Schadensausgleich im Innenverhältnis	592
d) Sonstige Nachteile	593
II. Management der Kartellrechtsrisiken in der Praxis	593
1. Risikoanalyse: Identifizierung und Bewertung	594
a) Kartellrechtliches Risikoprofil	594
b) Geschäftstätigkeit und Geschäftsbeziehungen	594
c) Risikokategorisierung und Risikobewertung	595
d) Einführung eines „Top down-Ansatzes“	596
2. Präventive Maßnahmen	596
a) Richt- und Leitlinien zum Kartellrecht	597
b) Schulungen (Präsenzschulungen und E-Learning)	599
3. Maßnahmen zur Kontrolle/Aufdeckung	601
III. Behördliche Untersuchungen	602
1. Durchsuchungen der EU-Kommission	603
a) Zuständigkeit	603
b) Befugnisse	604
c) Elektronische Durchsuchung	605
d) Typischer Ablauf	606

2.	Durchsuchungen des Bundeskartellamts	608
a)	Zuständigkeit	608
b)	Befugnisse	608
c)	Elektronische Durchsuchung	609
d)	Typischer Ablauf.	610
3.	Verhaltensregeln für die Unternehmen	611
a)	Vor der Durchsuchung	611
b)	Während der Durchsuchung	612
c)	Nach der Durchsuchung	613

21. Kapitel Datenschutz im Compliance-Management

	<i>(Becker/Böhlke/Fladung)</i>	615
I.	Einleitung.	615
II.	Der konzeptionelle Schutz personenbezogener Daten	618
1.	Gesetzliche Grundlagen.	618
a)	Bundesdatenschutzgesetz	618
b)	Landesdatenschutzgesetze	619
c)	Datenschutzgrundverordnung	619
d)	Europäische Richtlinien	620
e)	Weitere Gesetze mit datenschutzrechtlichen Vorgaben.	621
2.	Zentrale Grundsätze	623
a)	Verbot mit Erlaubnisvorbehalt.	623
b)	Prinzip der Verhältnismäßigkeit.	625
c)	Datensparsamkeit	626
d)	Transparenz	627
e)	Zweckbindung	627
3.	Grundbegriffe.	627
a)	Personenbezogene Daten	628
b)	Verantwortliche Stelle	629
c)	Umgang mit personenbezogenen Daten	629
aa)	Erheben	630
bb)	Verarbeiten	630
cc)	Nutzen.	632
d)	Auftragsdatenverarbeitung	633
III.	Betrieblicher Datenschutz.	634
1.	Pragmatischer Ansatz: Wo fange ich an?	634
2.	Beratungspraxis	637
a)	Der betriebliche Datenschutzbeauftragte	641
b)	Prozess der Datenschutzberatung	643
c)	Praxisrelevante Beispiele	646
3.	Implementierung	648
4.	Zusammenarbeit mit Behörden	651

Inhaltsverzeichnis

IV.	Instrumente der datenschutzrechtlichen Compliance.	652
1.	Tone-From-The-Top	652
2.	Interne Richtlinien	653
a)	Datenschutzrichtlinie	653
b)	IT-Nutzungsrichtlinie	654
c)	E-Mail-Policy	655
d)	IT-Datenschutzmanagement-Richtlinie (Datenschutzmanagementkonzept)	655
e)	Archivierungs- & Lösungsrichtlinie	656
3.	Verfahrensübersicht	657
4.	Verfahrensverzeichnis.	657
5.	Interne Kommunikation und Awareness	658
a)	Der Datenschutz-Newsletter	658
b)	Intranet	659
c)	Der Datenschutz-Tag & Fachtagungen	659
6.	Schulungen	659
a)	Persönliche Schulungen	660
b)	E-Learning/Webinars	661
c)	Unterstützung dezentraler Compliance-Funktionen. . .	662
V.	Effektive Datenschutzüberwachung	663
1.	Audits und Maßnahmepläne/Quick Self-Assessment. . . .	663
2.	IT-Infrastruktur-Reviews und Koordinierung mit IT Security	665
3.	Incident- und Regel-Reporting aus den Betrieben	666
4.	Der Datenschutzjahresbericht.	666
5.	Bericht an Aufsichtsrat/Compliance-Bericht/ Audit Committee	667
6.	Zusammenarbeit mit dem Compliance Officer, IT-Security & Revision	667
VI.	Beschäftigtendatenschutz	669
1.	Bedeutung des Beschäftigtendatenschutzes für Compliance	669
2.	Rechtsgrundlagen für den Umgang mit Mitarbeiterdaten	672
a)	Kollektivvereinbarungen zur Nutzung von Mitarbeiterdaten	672
b)	Rechtfertigende Einwilligung des Mitarbeiters	674
c)	Arbeitsvertragliche Regelungsmöglichkeiten	675
d)	Gesetzliche Erlaubnistatbestände	676
e)	Internationaler Datenverkehr mit Beschäftigtendaten. .	678

3.	Risiken beim Umgang mit Beschäftigtendaten	679
a)	Phase 1: Begründung des Arbeitsverhältnisses/ „Boarding-Phase“	679
b)	Phase 2: Durchführung des Arbeitsverhältnisses/ „On Board-Phase“	680
c)	Phase 3: Beendigung des Arbeitsverhältnisses/ „Off Boarding-Phase“	681
4.	Zusammenarbeit mit dem Betriebsrat.	682
5.	Personalleiter und Betriebsrat als Teil des Datenschutz- und Compliance-Teams	683
6.	Hinweise, Muster und Beispielfall	685
a)	Hinweise zur Regelung der Nutzung von Beschäftigtendaten	685
b)	Hinweise zur Regelung der Nutzung von Internet und E-Mail	686
c)	Beispielfall zur Kontrolle bei Verdacht gegen Mitarbeiter	689
VII.	Fazit	692

**22. Kapitel IT-Compliance – Software-Lizenzmanagement,
IT-Sicherheit und Blockchain**

	<i>(Jacobs)</i>	695
I.	Rechtliche Herausforderungen der fortschreitenden Digitalisierung und Vernetzung	695
II.	Software-Lizenzmanagement.	696
1.	Rechtliche Grundlagen der Nutzung von Computerprogrammen	697
2.	Besondere Arten von Software, insbesondere Open-Source-Software	698
3.	Software-Lizenzmanagement im Rahmen verantwortungsbewusster Unternehmensführung	699
4.	Rechtsfolgen einer Unterlizenzierung.	699
III.	Software-Lizenzmanagement im Rahmen von Cloud- Diensten	700
1.	Nutzungshandlungen beim Cloud Computing	700
a)	Recht der öffentlichen Zugänglichmachung der Software	701
b)	Recht zur Vervielfältigung der Software	702
2.	Lizenzmanagement im Zusammenhang mit Cloud Computing-Diensten	702

Inhaltsverzeichnis

IV.	Rechtsrahmen von Softwarelizenz-Audits	703
	1. Rechtliche Grundlagen für einen Softwarelizenz-Audit . . .	704
	2. Vertragliche Ausgestaltung eines Softwarelizenz-Audits . . .	705
V.	IT-Sicherheit	706
	1. Das IT-Sicherheitsgesetz	707
	a) Das BSIG	707
	aa) Adressatenkreis und Anwendungsbereich	707
	bb) Anforderungen an die Betreiber	708
	cc) Meldepflichten für Betreiber Kritischer Infrastrukturen	709
	dd) Der Begriff der Störung	710
	ee) Weitere Befugnisse des BSI	710
	ff) Sanktionsmöglichkeiten	710
	b) Änderungen im TKG	710
	aa) Sicherheitsanforderungen nach § 109 Abs. 2 Satz 2 TKG	711
	bb) Meldepflichten nach § 109 Abs. 5 TKG	711
	cc) Information der Nutzer nach § 109a TKG	711
	c) Änderungen im TMG	711
	d) Verhältnis zu NIS-Richtlinie	712
	2. Sonstige Quellen des Rechts der IT-Sicherheit	712
	a) Datenschutzrechtliche Anforderungen an die IT-Sicherheit	712
	b) Besondere Vorgaben für Banken/Finanzdienstleister/ Wertpapierdienstleistungsunternehmen und Versicherungsunternehmen	713
	c) Grundschutz-Katalog des BSI und internationale Normen	714
	3. Adressaten der Pflichten zur IT-Sicherheit	715
VI.	Blockchain und Smart Contracts	715
	1. Was ist die „Blockkette“?	716
	2. Rechtliche Herausforderungen und Compliance- Themen	716
VII.	Implementierung eines IT-Compliance-Systems	717
	1. Risikoanalyse und Grundlagen eines Lizenzmanagement- Systems	717
	2. Richtlinie zur IT-Sicherheit	719
	3. Der IT-Sicherheitsbeauftragte	719

23. Kapitel Cybersecurity, IT-Sicherheit und Krisenmanagement <i>(Bensinger)</i>	721
I. Analyse	721
1. Ziele der IT-Sicherheit	721
2. Cybercrime im Wandel	722
a) Ideelle Hintergründe	723
b) Materielle Hintergründe	724
3. Entwicklungen bei Schutzmaßnahmen	724
II. Vorbeugende Maßnahmen	725
1. Adressaten	725
a) KRITIS-Betreiber	726
b) Anbieter von Telemediendiensten	727
c) Anbieter von Telekommunikationsdiensten	727
d) Bank- und Finanzwesen	728
e) Energiewirtschaft	728
f) Geschäftsführung von Aktiengesellschaften und GmbHs	728
2. Inhalt der gesetzlichen Verpflichtungen	728
a) BSIG	729
b) BDSG	730
c) TMG	731
d) TKG	731
e) KWG, ZAG, MaRisk und MaSI	732
aa) MaRisk (Mindestanforderungen an das Risikomanagement)	732
bb) MaSI (Mindestanforderungen an die Sicherheit von Internetzahlungen)	733
cc) § 22 Abs. 1 ZAG	735
dd) Konkurrenz zum BSIG	735
f) EnWG	735
g) NIS-Richtlinie	736
h) §§ 76, 91, 93 AktG	737
3. Unternehmensinterne Vorkehrungen	738
a) Interne Vorgaben	738
b) Aktuelle technisch-organisatorische Schutzmaßnahmen	738
III. Der Krisenfall	739
1. Hacker-Angriffe erkennen	740
2. Rechtliche Konsequenzen und Handlungsoptionen.	740
a) Melde- und Informationspflichten	740
aa) BDSG	740

Inhaltsverzeichnis

bb) BSIG	741
cc) TMG	742
dd) TKG	742
ee) MaSI	743
ff) Sonstige Informationspflichten	743
b) Werkzeuge zur Abwehr von Cyberangriffen	743
3. Interne und externe Kommunikation	744
4. Mittel- und längerfristige Maßnahmen	745
IV. Ausblick	745
24. Kapitel Tax Compliance	
(Schwartz).	747
I. Einleitung	747
II. Steuerliche Pflichten	748
1. Allgemeine steuerliche Pflichten	748
2. Spezifische materiell-rechtliche Problemschwerpunkte	752
a) Lohnsteuer und Sozialabgaben	752
b) Umsatzsteuer	753
c) Verdeckte Gewinnausschüttungen.	754
d) Anzeigepflicht nach § 153 AO.	755
e) Tochtergesellschaften und Betriebstätten im Ausland.	757
f) Internationale Verrechnungspreise	758
g) Versagung des Betriebsausgabenabzugs nach § 160 AO	758
h) Betriebsausgabenabzugsverbot nach § 4 Abs. 5 Satz 1 Nr. 10 EStG	759
III. Risiken mangelnder Tax Compliance.	760
1. Steuerliche Haftungsrisiken.	760
2. Steuerstrafrechtliche und steuerordnungswidrigkeitenrechtliche Risiken	762
a) Sanktionen gegen Organe und Mitarbeiter	763
aa) Steuerhinterziehung und leichtfertige Steuerverkürzung (§§ 370, 378 AO)	763
(1) Täter	763
(2) Objektiver Tatbestand	764
(3) Subjektiver Tatbestand	767
(4) Strafe	769
bb) Verletzung der Aufsichtspflicht (§ 130 OWiG)	769
b) Sanktionen gegen das Unternehmen.	770
aa) Verbandsgeldbuße (§ 30 OWiG)	770
bb) Verfallsanordnung (§ 29a OWiG).	772

IV.	Tax Compliance-System	773
	1. Risikoanalyse	773
	2. Kernelemente eines Tax Compliance-Systems	774
	a) Zuständigkeit für Tax Compliance	774
	b) Zuständigkeit und Verantwortlichkeit bzgl. der steuerlichen Pflichten	774
	c) Berichtswege/Berichtspflichten	775
	d) Prozessbeschreibung Deklarationswesen	777
	e) Kontroll- und Überwachungsmaßnahmen.	778
	f) Umgang mit Betriebsprüfungen	779
	g) Schulungen	780
	h) Dokumentation	780
V.	Berichtigung von Steuererklärungen	781
	1. Korrekturvorschrift	781
	2. Selbstanzeige im Unternehmen (§§ 371, 378 Abs. 3 AO)	782
	a) Person des Anzeigerstatters	782
	b) Positive Wirksamkeitsvoraussetzungen des § 371 AO	782
	c) Negative Wirksamkeitsvoraussetzungen des § 371 AO (Sperrgründe)	785
	d) Absehen von Verfolgung nach § 398a AO.	787
	e) Bußgeldbefreiende Selbstanzeige nach § 378 Abs. 3 AO	789
VI.	Fazit.	789
25. Kapitel Exportkontrolle und Compliance		
	<i>(v. Bodungen)</i>	791
I.	Einleitung	791
II.	Rechtsgrundlagen der Exportkontrolle in Deutschland	792
	1. Supranationale Vorgaben	792
	2. Nationale Vorgaben	793
	3. Relevanz ausländischen Exportkontrollrechts	794
	a) Allgemeines	794
	b) Insbesondere: US-Re-Exportkontrolle.	794
III.	Exportkontrollrechtliche Genehmigungspflichten	796
	1. Allgemeines.	796
	2. Genehmigungspflichten bei Ausfuhren in Länder außerhalb der EU	796
	a) Gelistete Güter	796

Inhaltsverzeichnis

b) Nicht gelistete Güter	797
3. Genehmigungspflichten bei Verbringungen	798
a) Verbringungen bei Endverbleib in der EU.	798
b) Verbringungen mit anschließender Ausfuhr.	798
4. Sonstige Genehmigungspflichten	799
a) Handels- und Vermittlungsgeschäfte	799
b) Technische Unterstützung	800
IV. Exportkontrollrechtliches Genehmigungsverfahren	800
1. Zuständigkeit des BAFA	800
2. Ablauf des Genehmigungsverfahrens.	801
3. Genehmigungstypen	802
4. Sanktionen bei exportkontrollrechtlichen Verstößen	803
V. Exportkontrollrechtliche Compliance-Strukturen	804
1. Allgemeines	804
2. Der Ausführverantwortliche	805
3. Modell eines innerbetrieblichen Exportkontrollsystems	807
a) Überblick über die relevanten Strukturelemente	807
b) Umsetzung im Einzelfall	809
VI. Zusammenfassung	811
Literaturverzeichnis.	813
Stichwortverzeichnis	853