

INHALTSVERZEICHNIS

Vorwort	V
Autorenverzeichnis	VII
Inhaltsverzeichnis	IX
Abbildungsverzeichnis	XXI
Abkürzungsverzeichnis	XXIII
I. Ökonomische und rechtliche Bedeutung eines CMS nach IDW PS 980	1
1. Rechtliche Grundlage der Compliance	1
2. Ökonomische und rechtliche Bedeutung des CMS	3
3. Systematik des IDW PS 980 und seine Bedeutung für die Einrichtung eines CMS	4
4. Nutzen und Grenzen der CMS-Prüfung	7
5. Abgrenzung der Prüfung nach IDW PS 980 von anderen Standards	10
II. Elemente eines wirksamen Compliance-Management-Systems	13
1. Compliance-Kultur	13
1.1 Compliance-Kultur gem. IDW PS 980	13
1.2 Compliance-Kultur – unterschätzt und zugleich unerlässlich!	16
1.2.1 Verantwortung des Unternehmens	16
1.2.2 Mögliche Ausprägung der einzelnen Subelemente einer Compliance-Kultur	17
1.2.2.1 Top Management Commitment	18
1.2.2.2 Unternehmenskultur	20
1.2.2.3 Führung	20
1.2.2.4 Personalpolitik	21
1.2.2.5 Sanktionierung	22
1.2.2.6 Aufsichtsorgan	23
1.2.3 Konterkarierende Dynamiken im Unternehmen	23
1.2.3.1 Reduktion der Unsicherheit in illegalen Kooperationen	26
1.2.3.2 Beeinflussung zur Beteiligung an illegalen Aktivitäten	26
1.2.3.3 Sicherstellung der Geheimhaltung	26
1.3 Fazit: Change Management im Compliance-Management	26
2. Compliance-Ziele	29
2.1 Definition	29
2.2 Positionierung der Compliance-Ziele	30

2.2.1	Reputationsrisiken	31
2.2.2	Organhaftung	32
2.2.3	Außenwahrnehmung	32
2.3	Vorgehensweise	32
2.4	Geltungsbereich der Compliance-Ziele	35
2.5	Compliance-Ziele	36
2.6	Compliance-Ziele im ISO 19600	38
2.7	Rechtsgebiete als Teilbereiche eines CMS	38
2.7.1	Produktbezogenes CMS	38
2.7.1.1	Öffentlich-rechtliche Regelungen	39
2.7.1.2	Privatrechtliche Regelungen	40
2.7.1.3	Ausländische Regelungen	41
2.7.1.4	Risikoindikatoren	41
2.7.2	Korruption	42
2.7.2.1	Deutsches Korruptionsstrafrecht	42
2.7.2.2	Ausländisches Korruptionsstrafrecht	43
2.7.2.3	Risikoindikatoren	45
3.	Compliance-Risiken	46
3.1	Begriffsdefinition gem. IDW PS 980	46
3.2	Integration in das Risikomanagement und Auswirkungen auf das interne Kontrollsyste	46
3.2.1	Maßnahmen guter Corporate Governance	46
3.2.2	Risikomanagement-System	47
3.2.3	Internes Kontrollsyste	49
3.2.4	Auswirkungen von Compliance-Risiken auf das Risikomanagementsystem und das interne Kontrollsyste	51
3.3	Die rechtlichen Grundlagen eines Compliance Risk Assessments	54
3.3.1	Einleitung	54
3.3.2	Rechtliche Verpflichtung zur Durchführung eines Compliance Risk Assessments	54
3.3.3	Rechtlich verbindliche Anforderungen an die Ausgestaltung eines Compliance Risk Assessments	55
3.3.3.1	Reichweite	56
3.3.3.2	Compliance-Risiken	56
3.3.3.3	Interne Abstimmung	57
3.3.3.4	Methodik	57
3.3.3.5	Befragungsteilnehmer	58
3.3.3.6	Professionelle Durchführung	58
3.3.3.7	Sonstige Anforderungen	59
3.4	Praxisleitfaden für ein Compliance Risk Assessment	59
4.	Compliance-Programm	64
4.1	Der Begriff des Compliance-Programms	64

4.2	Überblick über unternehmensinterne Vorgaben (Selbstverpflichtungen, Richtlinien, Verhaltensstandards, Vorgaben von Geschäftspartnern)	65
4.2.1	Einleitung	65
4.2.2	Regelungsarten	66
4.2.3	Regelungsprozess	67
4.2.4	Gesellschaftsrechtliche Umsetzung von unternehmensinternen Regelungen	67
4.2.5	Arbeitsrechtliche Umsetzung von unternehmensinternen Regelungen	68
4.2.6	Datenschutzrechtliche Aspekte von unternehmensinternen Regelungen	70
4.2.7	Wirkung von unternehmensinternen Regelungen nach „außen“	70
4.3	Entwicklung des Compliance-Programms	71
4.3.1	Sinn und Zweck der Erstellung eines Compliance-Programms nach IDW PS 980	74
4.3.2	Maßnahmen zur Begrenzung von Compliance-Risiken	74
	4.3.2.1 Prävention: Vermeidung von Regelverstößen/Integration von Sicherungsmechanismen	74
	4.3.2.1.1 Interne Beratung/präventive Rechtsberatung	74
	4.3.2.1.2 Schulungsmaßnahmen	75
	4.3.2.1.3 Hinweisgebersystem	79
	4.3.2.1.4 Compliance-Kontrollen	79
4.4	Detektion: Aufdeckung von und Umgang mit Compliance-Verstößen	80
4.4.1	Aufdeckung von Compliance-Verstößen	80
4.4.2	Umgang mit Compliance Verstößen	81
4.4.3	Sanktionen	81
4.5	Ausgewählte Komponenten des Compliance-Programms	82
4.5.1	Geschäftspartner-Due-Diligence	82
4.5.2	Vertragsgestaltung/Compliance- bzw. Integritätsklausel/Code of Conduct	84
4.5.3	Hinweisgebersystem/Whistleblowing-System	85
4.5.3.1	Begriffsbestimmung	85
4.5.3.2	Methoden/Ausgestaltung	86
4.5.3.3	Whistleblowing-Guidelines/-Richtlinie	87
4.5.3.4	Gesetzliche Vorschriften zur Errichtung eines Hinweisgebersystems	88
4.6	Das Compliance-Programm im Rahmen der externen Prüfung	89
5.	Compliance-Organisation	93
5.1	Begriffsdefinition und Merkmale nach IDW PS 980	93

5.2	Zuordnung der Compliance-Verantwortung innerhalb des Unternehmens	94
5.2.1	Rechtsabteilung	95
5.2.2	Interne Revision	95
5.2.3	Personalabteilung	95
5.2.4	Compliance-Abteilung	95
5.2.5	Chief Governance Officer (CGO)	96
5.3	Organisationsformen	96
5.4	Bestandteile der Compliance-Organisation	98
5.4.1	Chief Compliance Officer	98
5.4.2	Exkurs: Haftung des CCO	100
5.4.3	Compliance-Committee	101
5.4.4	Ombudssystem	102
5.5	Positionierung der Compliance-Organisation	102
5.6	Ressourcenausstattungen	104
6.	Compliance-Kommunikation	106
6.1	Bedeutung der Kommunikation im CMS	106
6.1.1	Aufgaben und Ziele im Überblick	106
6.1.2	Compliance-Kommunikation als Grundelement im IDW PS 980	108
6.1.3	Compliance-Kommunikation i. S. d. ISO 19600	109
6.2	Grundpfeiler erfolgreicher Compliance-Kommunikation	112
6.2.1	Verankerung in Unternehmensleitbild und Wertekanon	113
6.2.2	Information und Akzeptanz	114
6.2.3	Informationskultur	115
6.2.4	Rolle der Unternehmensleitung	116
6.2.5	Nachhaltigkeit des Kommunikationskonzepts	118
6.3	Prozesse und Instrumente der Compliance-Kommunikation	119
6.3.1	Kommunikative Anforderungen an den Compliance-Kodex	120
6.3.2	Unternehmensrichtlinien und CMS	121
6.3.3	Ergänzende Kommunikationsmedien	123
6.3.4	Compliance-Intranet	123
6.4	Wissensaufbau zu Compliance	124
6.4.1	Schulungsprogramm	124
6.4.2	Präsenzschulungen und E-Learning	125
6.4.3	Beratungsangebot	127
6.5	Berichtspflichten und Berichtswege	128
6.5.1	Hinweisgebersysteme (Whistleblowing-Systeme)	128
6.5.2	Informationen für die Unternehmensleitung	129
6.5.3	Kommunikation mit dem Aufsichtsrat	131
6.6	Externe Compliance- und Krisenkommunikation	132
6.6.1	Compliance-Website	132

6.6.2	Informationen für Geschäftspartner	133
6.6.3	Externe Kommunikation über Compliance-Vorfälle und Krisenkommunikation	133
7.	Überwachung und Verbesserung von CMS	138
7.1	Anforderung an die CMS-Überwachung	138
7.1.1	Zielsetzung	138
7.1.2	Dokumentationserfordernis	139
7.1.3	Berichtspflichten und Reaktion bei Verstößen	139
7.1.4	Verbesserung und Anpassungen des Systems	140
7.2	Unterschied zwischen systemimmanenter Überwachung und externer Prüfung	140
7.3	Praktische Umsetzung der Anforderungen	142
7.3.1	Überwachungsmaßnahmen	142
7.3.2	Überwachungsintervalle	143
7.3.3	Überwachung der Rahmenbedingungen	144
7.3.4	Überwachung der Compliance-Kultur	145
7.3.5	Dokumentationsanforderungen	146
7.3.6	Reaktion auf festgestellte Schwächen des CMS	147
7.3.7	Scoping von Überwachungsmaßnahmen	148
7.4	Operative Verantwortung für die Überwachung – Interne Revision, CMS-Prüfer oder Self-Assessments	149
III.	Ausgewählte Teilespekte für erfolgreiches Compliance-Management	151
1.	Der Weg zur Prüfbereitschaft	151
1.1	Einleitung	151
1.2	Grundlegende Entscheidungen	152
1.2.1	Festlegung der Rechtsgebiete	152
1.2.2	Regionale Abgrenzung	152
1.2.3	Auswahl des Prüfungstyps	153
1.2.4	Festlegung des Stichtags bzw. des Wirksamkeitszeitraums	153
1.3	Durchführung einer Bestandsaufnahme	154
1.4	Anfertigen einer CMS-Beschreibung	155
1.5	Durchführung eines Readiness Reviews	156
2.	Angemessenheits- und Wirksamkeitsprüfung	159
2.1	Die drei Auftragsarten des IDW PS 980	159
2.2	Die Phasen einer Wirksamkeitsprüfung	161
2.3	Prüfungsplanung (inklusive Risk Assessment und Scoping)	164
2.3.1	CMS-Beschreibung, Wesentlichkeit und Prüfungsprogramm	164

2.3.2	Risikoorientierung	167
2.3.2.1	Kenntnisse über die Geschäftstätigkeit sowie das wirtschaftliche und rechtliche Umfeld des Unternehmens	167
2.3.2.2	Prüfung des Risk Assessments und Scoping	168
2.4	Prüfungs durchführung	169
2.4.1	Die Prüfung der Aussagen in der CMS-Beschreibung	170
2.4.2	Die Prüfung der Grundsätze und Maßnahmen hinsichtlich Angemessenheit und Wirksamkeit	171
2.5	Aggregation der Prüfungsfeststellungen und Berichterstattung	172
2.5.1	Auswertung und Aggregation der Prüfungsfeststellungen	172
2.5.2	Berichterstattung	173
3.	Empfehlungen zur Ausgestaltung eines CMS nach ISO 19600	174
3.1	Allgemeines	174
3.2	Strukturen und wesentliche Inhalte	175
3.2.1	Aufbau und Methodik	175
3.2.2	Anwendungsbereich und Compliance-Begriff	178
3.2.3	Inhaltliche Empfehlungen zur Ausgestaltung des CMS	178
3.2.3.1	Kontext der Organisation	179
3.2.3.2	„Leadership“	180
3.2.3.3	„Planning“	181
3.2.3.4	„Support“	181
3.2.3.5	„Operation“	182
3.2.3.6	„Performance Evaluation“	183
3.2.3.7	„Improvement“	184
3.3	ISO 19600 und IDW PS 980	184
3.4	Zusammenfassende Einschätzung	187
4.	Zusammenspiel von Werte- und Kontrollorientierung im Compliance-Management	190
4.1	Einleitung	190
4.2	Compliance-Kultur als Basis eines effektiven Compliance-Managements	192
4.3	Werte als Ergänzung des Kontrollsystems	193
4.4	Unterschiedliche Wahrnehmung in mittelständischen und großen Unternehmen	195
4.5	Synergieeffekte nutzen	196
4.6	Fazit	198
5.	Implementierung eines CMS in Unternehmen im internationalen Umfeld	201
5.1	Einführung	201
5.2	Anforderungen an ein internationales CMS	202
5.3	Handlungsfelder, Risiken und Erfolgsfaktoren	203
5.3.1	Compliance-Kultur	203
5.3.2	Compliance-Ziele	206

5.3.3	Compliance-Risiken	208
5.3.4	Compliance-Programm	210
5.3.5	Compliance-Organisation	212
5.3.6	Compliance-Kommunikation	213
5.3.7	Compliance-Überwachung und Verbesserung	214
5.4	Fazit	215
6.	Außenwirtschaftsrecht/Exportkontrolle	217
6.1	Einleitung	217
6.2	Compliance-Anforderungen	218
6.2.1	Aufbauorganisation	218
6.2.2	Ablauforganisation	219
6.2.2.1	Empfängerbezogene Exportkontrolle	219
6.2.2.2	Länderbezogene Exportkontrolle	222
6.2.2.3	Güterbezogene Exportkontrolle	223
6.2.2.4	Verwendungsbezogene Exportkontrolle	224
6.2.3	Weiterbildung	225
6.2.4	Überwachung	225
6.3	Eigenkontrollanzeige	226
6.4	Fazit	226
7.	Kartellrechts-Compliance	228
7.1	Bedeutender Baustein des Compliance-Managements	228
7.2	Kartellrechtliche Verbotsnormen	230
7.3	Aktuelle Fokus-Themen der Kartellrechts-Compliance im Unternehmen	233
7.3.1	Informationsaustausch anlässlich von „Wettbewerberkontakten“	234
7.3.2	Passive Involvierung, insbes. anlässlich von Verbandstreffen	234
7.3.3	Kooperationsprojekte, insbes. „überschießender“ Informationsaustausch	235
7.3.4	Beziehungen zu Vertriebspartnern und Händlern, insbes. indirekte „Resale Price Maintenance“	236
7.3.5	Missbrauch einer marktbeherrschenden Stellung	236
7.4	Aufsichtsmaßnahmen des Unternehmens	237
7.4.1	Monitoring der Wettbewerberkontakte	238
7.4.2	Standardverträge/-klauseln und Abstimmungsprozess mit der Rechtsabteilung	239
7.4.3	Compliance-/Aufsichtsgespräche	240
7.4.4	Kartellrechts-Audits in besonders risikogeneigten Bereichen	240
8.	Tax Compliance	243
8.1	Einleitung	243
8.2	Begrifflichkeiten	243
8.2.1	Corporate Compliance	243

8.2.2	Tax Compliance	244
8.2.3	Tax Risk Management	244
8.3	Funktionen der Tax Compliance	245
8.3.1	Steuergestaltende Funktion	245
8.3.2	Abwehrende Funktion	246
8.3.2.1	Vermeidung von steuerstrafrechtlichen Risiken	246
8.3.2.2	Vermeidung von Haftungsrisiken	246
8.3.2.3	Steuerstreit	247
8.3.2.4	Umgang mit Ermittlungsmaßnahmen	247
8.3.2.5	Begleitung von Außenprüfungen	248
8.3.2.6	Kontroll- und Informationsfunktion	248
8.3.3	Organisatorische Funktion	248
8.4	Allgemeine Non-Compliance-Risiken	249
8.4.1	Insbesondere: Steuerhinterziehung und Steuerverkürzung	249
8.4.2	Insbesondere: Steuerliche Nebenleistungen	250
8.4.3	Schätzung von Besteuerungsgrundlagen	250
8.4.4	Haftung	250
8.5	Schwerpunktthemen der Tax Compliance	250
8.5.1	Ertragsteuern	250
8.5.2	Umsatzsteuer	251
8.5.3	Lohnsteuer und Sozialabgaben	251
8.5.4	Spenden und Sponsoring (Hospitality)	252
8.5.5	Verrechnungspreise	253
8.5.6	Die wirtschaftliche Betätigung der öffentlichen Hand	254
8.6	Zur Implementierung eines Tax Compliance-Systems	254
8.7	Zusammenfassung	255
9.	Ausgewählte branchen- und segmentspezifische Besonderheiten	258
9.1	Unternehmensspezifische Ausrichtung des CMS	258
9.2	Unternehmenstypus und Compliance-Management	259
9.2.1	Börsennotierte Unternehmen	259
9.2.1.1	Die wesentlichen kapitalmarktrechtlichen Pflichten	260
9.2.1.2	Kapitalmarkt-Compliance	263
9.2.2	Konzerne	265
9.2.2.1	Rechtlicher Rahmen	265
9.2.2.2	Compliance-Systeme im Konzern	269
9.2.3	Familienunternehmen und Mittelstand	270
9.3	Branchenspezifische Compliance-Schwerpunkte	272
9.3.1	Finanzdienstleister	272
9.3.1.1	Einschlägige Regelungen	272
9.3.1.2	Auswirkungen auf ausgewählte Elemente des CMS	274

9.3.2	Versicherungsunternehmen	275
9.3.2.1	Einschlägige Regelungen	275
9.3.2.2	Auswirkungen auf ausgewählte Elemente des CMS	276
9.3.3	Pharma- und Medizinbranche	277
9.3.3.1	Einschlägige Regelungen	277
9.3.3.2	Auswirkungen auf ausgewählte Elemente des CMS	278
9.3.4	Energiewirtschaft	279
9.3.4.1	Einschlägige Regelungen	279
9.3.4.2	Auswirkungen auf ausgewählte Elemente des CMS	279
9.3.5	Bauwesen und Immobilienwirtschaft	279
9.3.5.1	Einschlägige Regelungen	279
9.3.5.2	Auswirkungen auf ausgewählte Elemente des CMS	280
9.3.6	Chemische Industrie	280
9.3.6.1	Einschlägige Regelungen	280
9.3.6.2	Auswirkungen auf ausgewählte Elemente des CMS	282
10.	Public Corporate Compliance – Besonderheiten des Compliance Managements in öffentlichen Unternehmen	287
10.1	Einführung	287
10.2	Thesen zur Entwicklung von Public Corporate Compliance	287
10.3	Fazit	298
11.	Die Prüfung branchenspezifischer Selbstverpflichtungen nach IDW PS 980 am Beispiel des GDV-Verhaltenskodex	301
11.1	Hintergrund	301
11.2	Inhalt des GDV-Verhaltenskodex	301
11.3	Prüfung des GDV-Verhaltenskodex nach IDW PS 980	302
11.4	Integration der Umsetzung des GDV-Verhaltenskodex in das CMS des Versicherungsunternehmens	303
11.5	Fazit	304
12.	Kompetenzorientierter Governance-Ansatz als organisatorische Neuausrichtung der Governance-Funktionen im Unternehmen	306
12.1	Einleitung	306
12.2	Herausforderungen bei der Implementierung eines integrierten Governance-Ansatzes in der Praxis	306
12.2.1	Aktueller Diskussionsstand	306
12.2.2	Aufbauorganisatorische Herausforderungen	307
12.2.3	Ablauforganisatorische Herausforderungen	308
12.2.4	Kulturelle Herausforderungen	308
12.3	Governance – Quo-vadis?	309
12.3.1	Notwendigkeit eines Paradigmenwechsels	309
12.3.2	Kompetenzorientierter Governance-Ansatz	309

12.3.2.1	Organisatorische Neuausrichtung der Governance-Funktionen	309
12.3.2.2	Aufbau und organisatorische Einordnung im Unternehmen	312
12.3.2.2.1	Gegenüber dem Vorstand und Aufsichtsrat	312
12.3.2.2.2	Gegenüber den operativen Geschäftseinheiten	313
12.3.2.2.3	Im Außenverhältnis	313
12.3.2.3	Rollen und Verantwortlichkeiten innerhalb einer Governance-Organisation	313
12.3.2.3.1	Chief Governance Officer	313
12.3.2.3.2	Governance-Experte	314
12.3.2.3.3	Governance-Pool-Mitarbeiter	315
12.4	Kritische Würdigung	315
13.	IT-Compliance	317
13.1	Datenschutz-Compliance	317
13.1.1	Der Schutz personenbezogener Daten als Teil des Compliance-Managements	317
13.1.2	Der Regelungsrahmen des Datenschutzrechts	318
13.1.3	Wesentliche Bausteine der Datenschutz-Compliance	319
13.1.3.1	Verbot mit Erlaubnisvorbehalt und Zweckbindung	319
13.1.3.2	Datenvermeidung und Datensparsamkeit	320
13.1.3.3	Das Verfahrensverzeichnis	320
13.1.3.4	Der betriebliche Datenschutzbeauftragte	321
13.1.3.5	Umgang mit Rechten der Betroffenen	322
13.1.3.6	Lösichung und Sperrung personenbezogener Daten	322
13.1.3.7	Technisch-organisatorische Maßnahmen	323
13.3.4	Implementierung des Datenschutzes in ein CMS	324
13.1.4.1	Implementierung in ein CMS nach IDW PS 980	324
13.2	Incident-Response im CMS	327
13.2.1	Incident-Response als Teil des CMS	327
13.2.2	Ausgestaltung und Implementierung des Incident-Response-Systems im Lichte des PS 980	329
13.2.2.1	Incident-Response Kultur	329
13.2.2.2	Ziele	329
13.2.2.3	Risiken	330
13.2.2.4	Programm	330
13.2.2.4.1	Definition der rechtlichen Rahmenbedingungen	331
13.2.2.4.2	Definition des Prozesses	331
13.2.2.5	Organisation	334

13.2.2.6	Kommunikation	335
13.2.2.6.1	Interne Kommunikation	335
13.2.2.6.2	Externe Kommunikation	337
13.2.2.7	Überwachung und Verbesserung	337
14.	Compliance-Herausforderungen bei M&A-Transaktionen	339
14.1	Einleitung	339
14.2	Ablauf einer M&A-Transaktion	339
14.3	Compliance-Herausforderungen bei der Durchführung einer M&A-Transaktion	340
14.3.1	Compliance bei der Entscheidung über die Durchführung der Transaktion	340
14.3.2	Compliance bei der Preisgabe von vertraulichen Informationen	341
14.3.3	Kartellrechtliche Compliance bei der Durchführung der Transaktion	342
14.3.4	Definierte Prozessabläufe zur Sicherstellung von Compliance-Vorgaben	343
14.4	Compliance Due Diligence bei M&A-Transaktionen	343
14.4.1	Funktionen der Compliance Due Diligence	344
14.4.2	Informationsgrundlage der Compliance Due Diligence	345
14.5	Compliance bei Post Merger Integration	347
15.	Die Rolle der zentralen und dezentralen Compliance Officer in der Überwachung	350
15.1	Einführung	350
15.2	Organisatorische Abbildung der Überwachungsfunktion	350
15.3	Einbindung der Internen Revision in die Überwachung des CMS	351
15.4	(Selbst-)Überwachungsmaßnahmen der Compliance-Abteilung	351
15.5	Überwachungsmöglichkeiten für ausgewählte Elemente des CMS	352
15.6	Compliance-IKS als Instrument der kontinuierlichen Überwachung der Wirksamkeit des CMS	353
16.	CMS-Beschreibung als Grundlage für die Überwachung durch Vorstand und Aufsichtsrat	356
16.1	Einleitung	356
16.2	Informationspflichten	357
16.3	Aufbau und Inhalt einer CMS-Beschreibung	357
16.3.1	Compliance-Ziele	358
16.3.2	Compliance-Kultur	360
16.3.3	Compliance-Risiken	361
16.3.4	Compliance-Programm	363
16.3.5	Compliance-Organisation	364
16.3.6	Compliance-Kommunikation	365
16.3.7	Compliance-Überwachung und Verbesserung	366
16.4	Umfang und Tiefe der Beschreibung	367
16.5	Fazit	368

IV. Zusammenfassung	371
1. Welche ökonomische und rechtliche Bedeutung kommt dem CMS zu?	371
2. Welche Relevanz kommt den Elementen eines wirksamen CMS im Sinne des IDW PS 980 zu?	372
3. Welche Teilspekte machen ein erfolgreiches Compliance-Management aus?	375
Stichwortverzeichnis	385