

Inhaltsverzeichnis

Einleitung	V
Literaturverzeichnis	XV

1. Kapitel. Praktische Einführung

1. Grundlagen der Compliance	1
1.1. Bezugspunkt der Compliance	2
1.2. Compliance als Wertschöpfung und Mehrwert	3
1.3. Entwicklung	4
1.4. Motivation für die Einführung	4
1.4.1. Allgemein	4
1.4.2. Originäre Organisationspflicht	7
1.4.3. Im Mittelstand	8
2. Entwicklung globaler Compliance-Standards	8
2.1. ISO-Managementnormen im Allgemeinen	8
2.2. DIN ISO 19600 Compliance Management-Systems	10
2.2.1. Initiative	10
2.2.2. Arbeit am Standard	11
2.2.3. Allgemeine Merkmale	12
2.3. ISO 37001 Anti-Bribery Management-Systems	13
2.3.1. Entstehung und Hintergründe	13
2.3.2. Allgemeine Merkmale	13
2.3.3. Verhältnis zwischen ISO 37001 und DIN ISO 19600	14
2.3.4. Anwendung beider Normen in der Praxis	14
2.4. Weitere Normungsaktivitäten – der Ausblick	15
3. Grundbegriffe und Anwendbarkeit	16
3.1. Grundbegriffe	16
3.1.1. Compliance	16
3.1.2. Bindende Verpflichtungen	17
3.1.3. Compliance-Management-System	18
3.1.4. Compliance-Funktion (Compliance-Officer)	19
3.1.5. Weitere wesentliche Begriffe nach ISO 37001	20
3.1.6. Mittelstand	21
3.1.7. Begriffliche Abgrenzung	21
3.2. Nachhaltige Compliance-Kultur (Wertebasiertes CMS)	25
3.2.1. Begriff der Compliance-Kultur	25
3.2.2. Herausforderungen in multikulturellen Organisationen	29
3.2.3. Compliance-Kultur und Mittelstand	31
3.3. Anwendbarkeit der Standards	31
3.3.1. Universeller Geltungsanspruch	32
3.3.2. Referenzrahmen für Justiz und sonstige Anwender	33
4. Funktionen und Ziele eines CMS	36
4.1. Zielsetzung	36
4.1.1. Ziele eines CMS	36
4.1.2. Ziele der ISO-Managementnormen	36
4.2. Funktionen	37
4.2.1. Allgemeine Anmerkungen	37
4.2.2. Prävention	37

4.2.3. Repression	38
4.2.4. Gemischte Funktionen	40
4.2.5. Funktionale Ansätze in der Praxis	42
4.2.6. Funktionen mittelständischer Compliance	43
5. CMS in besonderen Organisationsarten	43
5.1. Mittelständische Compliance	43
5.1.1. Allgemeine Anmerkungen	43
5.1.2. Ausgangslage: Spannungsfeld und Herausforderungen	44
5.1.3. Tauglichkeit und Nutzung der ISO-Standards	46
5.1.4. Kostenorientierte Implementierung	48
5.1.5. Besondere Vorteile	49
5.2. Öffentliche Verwaltung	50
6. Unbegründete Kritik am DIN ISO 19600	51
6.1. Pauschale Kritikpunkte	51
6.2. Kritikpunkte im Einzelnen	52
6.2.1. Entstehungsverfahren	52
6.2.2. Vergleichbarkeit trotz landesspezifischer Abweichungen	52
6.2.3. Verhältnis zwischen DIN ISO 19600 und ISO 37001	53
6.2.4. Belastung für den Mittelstand	53
6.2.5. Vereinbarkeit mit anderen Normen, insbes. IDW PS 980	54

2. Kapitel. CMS-Modelle und Grundgestaltung

7. CMS-Gestaltungsgrundsätze	57
7.1. Prinzip von Good Governance	58
7.2. Verhältnismäßigkeit	58
7.2.1. Bedeutung	58
7.2.2. Funktionsweise	60
7.2.3. Mittelstand	61
7.3. Transparenz	61
7.4. Nachhaltigkeit	63
7.5. Flexibilität	63
7.5.1. Bedeutung	63
7.5.2. Mittelstand	64
7.6. Weitere Grundsätze	64
7.6.1. Wirtschaftlichkeitsgrundsatz (Effizienz)	64
7.6.2. Integrationsgrundsatz	64
7.6.3. Einbeziehungsgrundsatz (Akzeptanz)	66
7.6.4. Vorrang des Rechts	67
8. CMS-Grundmodelle	67
8.1. CMS-Modell in den ISO-Normen	67
8.1.1. High Level Structure (HLS)	67
8.1.2. Risk-Management-System (RMS)	69
8.1.3. PDCA-Modell	70
8.1.4. Zusammenführung der Modelle	72
8.2. Weitere CMS-Modelle im Vergleich	73
8.2.1. Mittelständische Compliance	73
8.2.2. IDW PS 980	73
8.2.3. Vorschläge der Verbände	74
8.2.4. Vergleichbarkeit	76

9. Grundphasen eines CMS	77
9.1. Allgemeine Anmerkungen	77
9.2. Vier Grundphasen im Einzelnen	78
9.2.1. Einrichtung (PLAN), Schritte 1/8–3/8	78
9.2.2. Implementierung (DO), Schritte 4/8–6/8	79
9.2.3. Leistungsprüfung (CHECK), Schritt 7/8	79
9.2.4. Verbesserung (ACT), Schritt 8/8	80
9.3. Grundphasen im Mittelstand	80
 3. Kapitel. Vier Phasen der CMS-Implementierung	
Abschnitt I: Einrichtung (PLAN)	
10. Kontext der Organisation, inkl. Risikosteuerung (Schritt 1/8)	82
10.1. Organisation	83
10.1.1. Allgemeine Empfehlungen nach DIN ISO 19600	83
10.1.2. Weitere Anforderungen nach ISO 37001	83
10.2. Interessierte Parteien	84
10.3. Bindende Verpflichtungen	85
10.3.1. Begrifflichkeiten	85
10.3.2. Systematische Einordnung und Unterschiede	85
10.3.3. Ermittlung von bindenden Verpflichtungen	86
10.3.4. Aktualisierung	87
10.3.5. Mittelstand	88
10.4. Compliance-Risk-Management (CRM)	88
10.4.1. Allgemeine Bedeutung	88
10.4.2. Begrifflichkeiten und systematische Einordnung	89
10.4.3. Empfehlungen der DIN ISO 19600	90
10.4.4. Grundsätze der Risikoverwaltung nach ISO 31000	92
10.4.5. CRM im Mittelstand	93
10.4.6. Besonderheiten eines AMS	94
10.5. Anwendungsbereich des CMS	94
10.5.1. Sachlicher Anwendungsbereich	94
10.5.2. Funktionaler Anwendungsbereich	96
10.5.3. Räumlicher Anwendungsbereich	96
10.5.4. Anwendungsbereich im Mittelstand	98
10.5.5. Integration und Zentralisierung	98
10.6. Mittelstand	100
10.7. Anforderungen nach ISO 37001	100
11. Rolle der Führung (Schritt 2/8)	100
11.1. Bedeutung	100
11.2. Begriffe	101
11.2.1. Oberste Leitung (<i>top management</i>)	101
11.2.2. Führungsgremium (<i>governing body</i>)	101
11.2.3. Abgrenzung und Handhabung	101
11.3. Führung als „Ermöglicher“	102
11.4. Klares Bekenntnis und aktive Unterstützung	102
11.4.1. Festlegen	103
11.4.2. Sicherstellen	104
11.4.3. Kommunizieren	105
11.4.4. Sensibilisieren	105
11.5. Indikatoren für die Qualität des Bekenntnisses	108
11.6. Mittelstand	109

11.7. Anforderungen nach ISO 37001	110
12. Compliance-Politik (Schritt 3/8)	110
12.1. Grundlagen	110
12.2. Entwicklung der Compliance-Politik	111
12.2.1. Verfasser der Compliance-Politik	111
12.2.2. Bedeutung der Einbeziehung von Organisationsmitgliedern	112
12.2.3. Zu beachtende Aspekte	112
12.2.4. Aktualisierung	113
12.3. Inhalte	113
12.3.1. Anwendungsbereich des CMS	114
12.3.2. Integration des CMS	114
12.4. Form	114
12.5. Mittelstand	115
12.6. Antikorruptions-Politik nach ISO 37001	115

Abschnitt II: Implementierung (DO)

13. Klare Rollenzuweisung (Schritt 4/8)	116
13.1. Bedeutung für das CMS	116
13.2. Führung	117
13.3. Compliance-Funktion (Compliance-Manager)	117
13.3.1. Bedeutung und Begriffe	117
13.3.2. Grundlagen	118
13.3.3. Flexible Ausgestaltung	120
13.3.4. Ausgewählte Aufgabenbereiche	120
13.3.5. Fähigkeiten der Compliance-Funktion	124
13.3.6. Compliance-Funktion für Korruptionsbekämpfung (ISO 37001)	125
13.3.7. Mittelstand	126
13.3.8. Auslagerung der Compliance- und Anti-Bribery Funktion	127
13.4. Manager	128
13.4.1. Auch Manager verantworten Compliance	128
13.4.2. Flexible Ausgestaltung der Managerrolle für Compliance	129
13.4.3. Konkrete Compliance-Aufgaben der Manager	129
13.4.4. Manager-Aufgaben gegen Korruption nach ISO 37001	132
13.5. Mitglieder der Organisation (zB alle Beschäftigten)	132
13.5.1. Herausforderung	132
13.5.2. Aufgabenkatalog	132
13.6. Umsetzung der Rollenzuordnung	134
13.6.1. Delegierung	134
13.6.2. Kommunikation und Unterstützung	135
13.6.3. Anforderungen nach ISO 37001	135
14. Planung (Schritt 5/8)	135
14.1. Grundlagen der Planung	136
14.2. Informationen als Basis für die Planung	136
14.3. Inhalte des Plans	137
14.4. Plan nach ISO 37001	138
15. Unterstützung – Umsetzung von Compliance-Maßnahmen (Schritt 6/8)	138
15.1. Personelle und finanzielle Ressourcen	138
15.1.1. Umfang der Ressourcen	138
15.1.2. Arten der Ressourcen	139
15.1.3. Grenzen	139

15.2. Compliance-Kommunikation	139
15.2.1. Bedeutung der Compliance-Kommunikation	140
15.2.2. Grundlagen der Compliance-Kommunikation	141
15.2.3. Sensibilisierung und Compliance-Bewusstsein	143
15.2.4. Compliance-Anreize	144
15.2.5. Sonderfall: Hinweisgebersysteme (Whistleblowing)	145
15.3. Nachhaltige Compliance-Kultur im Mittelpunkt	152
15.3.1. Systematische Einordnung	152
15.3.2. Methoden zur Förderung der Compliance-Kultur	153
15.3.3. Indikatoren für das Vorhandensein der Compliance-Kultur	156
15.3.4. Antikorruptionskultur in ISO 37001	157
15.4. Kompetenzsteigerung und Schulungen	158
15.4.1. Kompetenzsteigerung	158
15.4.2. Schulung	160
15.4.3. Mittelstand	164
15.4.4. Anforderungen der ISO 37001	164
15.5. Betrieb (Operation)	166
15.5.1. Betriebliche Planung und Steuerung	166
15.5.2. Integration in das bestehende Betriebsumfeld	167
15.5.3. Externe Prozesse	168
15.6. Sondermaßnahmen gegen Korruption (ISO 37001)	168
15.6.1. Due Diligence (korruptionsrelevante Prüfungen)	169
15.6.2. Finanzielle und nichtfinanzielle Kontrollen	170
15.6.3. Antikorruptionskontrollen durch Dritte	170
15.6.4. Compliance-Bekanntnis der Geschäftspartner	171
15.6.5. Umgang mit Geschenken, Einladungen und anderen Vorteilen	171
15.6.6. Hinweisgebersysteme und Ermittlungen	172
15.6.7. Mittelstand	173
15.7. Verhaltenskodex (VK)	173
15.7.1. Bedeutung des Verhaltenskodexes im Rahmen eines CMS	173
15.7.2. Empfehlungen der DIN ISO 19600 und Abgrenzung	173
15.7.3. Funktionen	174
15.7.4. Konzipierung	174
15.7.5. Grundsätze der Gestaltung und Umsetzung	176
15.7.6. Mittelstand	177
15.8. Compliance-Dokumentation	177
15.8.1. Informationen als Ausgangsbasis	177
15.8.2. Bedeutung und Begriffe	178
15.8.3. Umfang und Gegenstand der Dokumentation	180
15.8.4. Verwaltung von Informationen	182
15.8.5. Aufzeichnungen	184
15.8.6. Dokumentation nach ISO 37001	185
15.8.7. Compliance-Dokumentation im Mittelstand	186
15.9. Berichterstattung	186
15.9.1. Allgemeine Bedeutung	186
15.9.2. Berichterstattung	186
15.9.3. Meldewesen (Hinweisgebersysteme)	189

Abschnitt III: Leistungsprüfung (CHECK)

16. Bewertung (Schritt 7/8)	189
16.1. Allgemeine Bedeutung der CMS-Bewertung	189
16.1.1. Funktionen der Leistungsprüfung	190

16.1.2. Systematik der Prüfungsmethoden	191
16.2. Leistungsprüfung nach DIN ISO 19600 und ISO 37001	192
16.2.1. Planung, insbes. Gegenstände der Überwachung	192
16.2.2. Überwachung (Informationsbeschaffung)	194
16.2.3. Bewertung	197
16.2.4. Sonderfall: Prüfung der Effektivität des CMS	197
16.3. Audit	198
16.3.1. Begriffe und allgemeine Bedeutung	198
16.3.2. Planung und Durchführung	199
16.3.3. Interner Audit nach ISO 37001	201
16.4. Überwachung durch die Führung	202
16.4.1. Bewertungsaspekte	203
16.4.2. Bewertungsergebnisse und Optimierungsempfehlungen	203
16.4.3. Besonderheiten nach ISO 37001	204
16.5. Mittelstand	204

Abschnitt IV: Verbesserung (ACT)

17. Verbesserung (Schritt 8/8)	204
17.1. Einleitung	205
17.2. Compliance-Krisenmanagement	206
17.2.1. Grundlagen	206
17.2.2. Effektive Aufklärung (interne Ermittlungen)	208
17.2.3. Reaktionen	211
17.2.4. Kommunikation über Compliance-Verfehlungen	214
17.2.5. Dokumentation und Bedeutung der Ergebnisse	214
17.3. Ständige CMS-Verbesserung	215
17.3.1. Bedeutung	215
17.3.2. Integrierte Dauerverbesserung	215
17.4. Mittelstand	218
17.5. Anforderungen nach ISO 37001	218
Zusammenfassung	219