

Inhaltsverzeichnis

Vorwort 5

Abbildungsverzeichnis 13

Tabellenverzeichnis 13

I. Grundsätzliches zu Compliance 15

1. ISO 19600 – Ein offener und flexibler Standard in einem normierten Kontext. 15

2. Entwicklung des ISO 19600 Compliance-Management-Systems 23

3. Der Begriff Compliance und seine Bedeutung 25

4. Der Risiko-Management-Ansatz von ISO 31000 im neuen ISO 19600 27

5. Auf dem Weg zur Standardisierung: Über IDW PS 980 zu ISO 19600 33

6. Nationale und internationale Standards im Überblick 40

7. Die Entwicklung der Rechtsprechung zu Haftung und Compliance – Von Utz Claassen zu Heinz-Joachim Neubürger 43

8. Hilft ISO 19600 dabei, Strafen zu mildern und Haftung zu vermeiden? 51

II. Inhalte und Grundsätze von ISO 19600 53

1. Geltungsbereich 53

2. Normative Verweise 54

3. Begriffe und Definitionen 54

4. Kontext der Organisation 58

4.1 Verstehen der Organisation und deren Kontext 58

4.2 Verstehen der Bedürfnisse und Erwartungen der interessierten Parteien 59

4.3 Bestimmung des Geltungsbereichs des CMS 60

4.4 CMS und die Grundsätze der guten Unternehmensführung ... 60

4.5 Compliance-Verpflichtungen 62

4.5.1 Identifikation von Compliance-Verpflichtungen 63

4.5.2 Aufrechterhaltung von Compliance-Verpflichtungen 65

4.6	Identifikation, Analyse und Bewertung von Compliance-Risiken	66
5.	Leitung	73
5.1	Führung und Selbstverpflichtung	73
5.2	Compliance-Grundsätze	80
5.2.1	Allgemein	80
5.2.2	Entwicklung	84
5.3	Organisatorische Aufgaben, Verantwortlichkeiten und Befugnisse	86
5.3.1	Allgemein	86
5.3.2	Zuordnung von Verantwortlichkeiten der Organisation	87
5.3.3	Rolle und Verantwortung von Vorstand und Top- Management	88
5.3.4	Compliance-Funktion	91
5.3.5	Verantwortung des Managements	102
5.3.6	Verantwortung der Mitarbeiter	106
6.	Planung	107
6.1	Maßnahmen zur Bewältigung von Compliance-Risiken	107
6.2	Compliance-Ziele und Planung ihrer Erreichung	109
7.	Support/Unterstützung	112
7.1	Ressourcen	112
7.2	Kompetenz und Schulung	113
7.2.1	Kompetenz	114
7.2.2	Schulung	128
7.3	Sensibilisierung/Bewusstseinsbildung	130
7.3.1	Allgemein	130
7.3.2	Verhaltensweisen	131
7.3.2.1	Allgemein	131
7.3.2.2	Die Rolle des Managements bei der Förderung von Compliance	131
7.3.2.3	Compliance-Kultur	132
7.4	Kommunikation	137
7.4.1	Allgemein	137
7.4.2	Interne Kommunikation	138
7.4.3	Externe Kommunikation	140
7.5	Dokumentierte Informationen	141
7.5.1	Allgemein	142
7.5.2	Anlegen und Aktualisieren	143
7.5.3	Kontrolle der dokumentierten Informationen	144
8.	Arbeitsablauf	146
8.1	Operative Planung und Steuerung	146

8.2	Einrichtung interner Kontrollen und Verfahren	147
8.3	Ausgegliederte Prozesse	152
9.	Leistungsbewertung	153
9.1	Überwachung/Monitoring, Messung, Analyse und Bewertung	153
9.1.1	Allgemein	154
9.1.2	Überwachung	155
9.1.3	Quellen für Feedback über Compliance-Leistung	156
9.1.4	Methoden der Informationserfassung	157
9.1.5	Informationsanalyse und Klassifizierung	158
9.1.6	Entwicklung von Indikatoren	159
9.1.7	Compliance-Reporting/Berichterstattung	160
9.1.8	Inhalt von Compliance-Berichten	163
9.1.9	Protokollierung	164
9.2	Prüfung/Audit	165
9.3	Managementauswertung	167
10.	Verbesserung	168
10.1	Nichtkonformität, Non-Compliance und korrigierende Maßnahmen	168
10.1.1	Allgemein	168
10.1.2	Eskalation	170
10.2	Kontinuierliche Verbesserung	171
III.	Die Zertifizierung nach ISO 19600.	173
1.	Wer darf zertifizieren?	174
2.	Was wird zertifiziert?	175
3.	Ablauf der Zertifizierung	176
4.	Audit der Stufe 2	177
5.	Abweichung von den Voraussetzungen	178
6.	Auditbericht zur Erstzertifizierung nach Stufe 1	179
7.	Auditbericht zur Erstzertifizierung der Stufe 2	179
8.	Entscheidung über die Zertifizierung	180
9.	Erneute Zertifizierung	180
IV.	Checklisten	181
1.	ISO-Checklisten	181
2.	ISO-Checklisten mit Zertifizierung	226
3.	Zertifizierungs-Check	282
4.	Kontext der Organisation	283
4.1	Verstehen der Organisation und deren Kontext	283

4.2	Verstehen der Bedürfnisse und Erwartungen der interessierten Parteien.....	283
4.3	Bestimmung des Geltungsbereichs des CMS.....	283
4.4	CMS und die Grundsätze der guten Unternehmensführung....	283
4.5	Compliance-Verpflichtungen.....	283
4.5.1	Identifikation von Compliance-Verpflichtungen.....	283
4.5.2	Aufrechterhaltung von Compliance-Verpflichtungen.....	283
4.6	Identifikation, Analyse und Bewertung von Compliance-Risiken.....	283
5.	Leitung.....	284
5.1	Führung und Selbstverpflichtung.....	284
5.2	Compliance-Grundsätze.....	284
5.2.1	Allgemein.....	284
5.2.2	Entwicklung.....	284
5.3	Organisatorische Aufgaben, Verantwortlichkeiten und Befugnisse.....	285
5.3.1	Rolle und Verantwortung von Vorstand und Top-Management.....	285
5.3.2	Compliance-Funktion.....	285
5.3.3	Verantwortung des Managements.....	285
5.3.4	Verantwortung der Mitarbeiter.....	286
6.	Planung.....	286
6.1	Maßnahmen zur Bewältigung von Compliance-Risiken.....	286
6.2	Compliance-Ziele und Planung ihrer Erreichung.....	286
7.	Support/Unterstützung.....	286
7.1	Ressourcen.....	286
7.2	Kompetenz und Schulung.....	287
7.2.1	Kompetenz.....	287
7.2.2	Schulung.....	287
7.3	Sensibilisierung.....	287
7.3.1	Allgemein.....	287
7.3.1.1	Die Rolle des Managements bei der Förderung von Compliance.....	288
7.3.1.2	Compliance-Kultur.....	288
7.4	Kommunikation.....	288
7.4.1	Allgemein.....	288
7.4.2	Interne Kommunikation.....	288
7.4.3	Externe Kommunikation.....	288
7.5	Dokumentierte Informationen.....	288
7.5.1	Allgemein.....	288
7.5.2	Anlegen und Aktualisieren.....	289
7.5.3	Kontrolle der dokumentierten Informationen.....	289

8.	Arbeitsablauf	289
8.1	Operative Planung und Steuerung	289
8.2	Einrichtung interner Kontrollen und Verfahren	289
8.3	Ausgegliederte Prozesse	290
9.	Leistungsbewertung	290
9.1	Überwachung/Monitoring, Messung, Analyse und Bewertung	290
9.1.1	Allgemein	290
9.1.2	Überwachung	290
9.1.3	Quellen für Feedback über Compliance-Leistung	290
9.1.4	Informationsanalyse und Klassifizierung	290
9.1.5	Entwicklung von Indikatoren	290
9.1.6	Compliance-Reporting/Berichterstattung	291
9.1.7	Inhalt von Compliance-Berichten	291
9.1.8	Protokollierung	291
9.2	Prüfung/Audit	291
9.3	Managementauswertung	292
10.	Verbesserung	292
10.1	Nichtkonformität, Non-Compliance und korrigierende Maßnahmen	292
10.1.1	Allgemein	292
10.1.2	Eskalation	292
10.2	Kontinuierliche Verbesserung	292
	Literaturverzeichnis	293