

KPMG AG Wirtschaftsprüfungsgesellschaft (Hrsg.)

Compliance Management im Wandel

Ein Praxisleitfaden für die Einrichtung eines ganzheitlichen CMS

- ▶ CMS nach IDW PS 980
- ▶ Integration ausgewählter Teilrechtsgebiete in das CMS
- ▶ Praxishinweise



cutting through complexity

▶ **nwb** E-BOOK

KPMG AG Wirtschaftsprüfungsgesellschaft (Hrsg.) ·
Compliance Management im Wandel

Compliance Management im Wandel

Ein Praxisleitfaden für die Einrichtung eines
ganzheitlichen CMS

- ▶ CMS nach IDW PS 980
- ▶ Integration ausgewählter Teilrechtsgebiete in das CMS
- ▶ Praxishinweise

Herausgegeben von der
KPMG AG Wirtschaftsprüfungsgesellschaft

ISBN 978-3-482-**67691**-8
eISBN 978-3-482-01411-6

© NWB Verlag GmbH & Co. KG, Herne 2020
www.nwb.de

Alle Rechte vorbehalten.

Dieses Werk und alle in ihm enthaltenen Beiträge und Abbildungen sind urheberrechtlich geschützt. Mit Ausnahme der gesetzlich zugelassenen Fälle ist eine Verwertung ohne Einwilligung des Verlages unzulässig.

Satz: PMGi Agentur für intelligente Medien GmbH, Hamm
Druck: CPI books, Leck

GRÜßWORT

Das Compliance Management System (CMS) ist und bleibt der wesentliche Treiber in der Diskussion rund um die gute Unternehmensführung (Corporate Governance). Die Frage, wie eine angemessene Aufbau- und Ablauforganisation geschaffen werden kann, die die relevanten rechtlichen Teilbereiche und die darin enthaltenen Risikoszenarien identifiziert und bewertet, um ausgehend von dieser Analyse geeignete und wirksame Compliance Maßnahmen einzurichten, ist für jedes Unternehmen hochgradig relevant. Es spielt keine Rolle mehr, ob es sich um börsennotierte Unternehmen oder Familienunternehmen handelt, die Regulatorik und die Anforderungen der internationalen Zusammenarbeit machen hier keine nennenswerten Unterschiede mehr.

Dabei geht es schon lange nicht mehr nur um Anti-Korruption oder Kartellrecht. Die anhaltende Diskussion um das Steuer IKS bzw. Tax CMS, die Datenschutzgrundverordnung, Geldwäsche- und Sanktionsanforderungen sind hinzugekommen. Die Herausforderung Produkte nachweislich nur in den Markt zu bringen, wenn Abgasvorschriften oder vereinfacht Produktqualitätsanforderungen eingehalten sind, erweitert wiederum das CMS. Und im Zuge der Nachhaltigkeitsinitiativen der UN und zuletzt verstärkt der EU rücken Menschenrechte, Umweltschutz und Arbeitssicherheit genauso in den Fokus des CMS, wie ein angemessenes Lieferkettenmanagement.

Mitten in der Coronakrise – am 21.4.2020 – hat das Bundesministerium der Justiz und für Verbraucherschutz (BMJV) den Referentenentwurf zum sog. Verbandssanktionengesetz (Gesetz zur Stärkung der Integrität in der Wirtschaft, VerSanG-E) veröffentlicht. Damit wird die Frage, ob ein CMS im Haftungsfall sanktionsmildernd wirken kann, voraussichtlich bejaht, ebenso wie die Anforderung, ein CMS einrichten zu müssen.

Die alles entscheidende Frage, wie das CMS nun einzurichten ist, bleibt hingegen gesetzlich unbeantwortet und somit Bestandteil der öffentlichen Diskussion. Das ist einerseits begrüßenswert, da so die individuelle Begebenheit des Unternehmens berücksichtigt werden kann. Gleichwohl gilt auch: Ein formell zugekauft Compliance Programm bzw. ein Papiertiger, der weder akzeptiert noch gelebt wird, kann nicht als „angemessen“ bewertet werden und wird voraussichtlich auch keine nennenswerte Sanktionsmilderung mit sich bringen.

Wie also geht das nun, ein „angemessen und wirksames CMS“ einzurichten? Es gibt nicht das eine CMS, das standardisiert zu implementieren ist und zu jedem Unternehmen passt. Es darf erwartet werden, dass Unternehmen ihrer Sorgfaltspflicht zur CMS Einrichtung dahingehend nachkommen, dass sie sich mit den für ihr Unternehmen relevanten Themenfeldern und Szenarien auseinandersetzen und dies auch dokumentieren. Dazu gehört sicher auch, zu verstehen und zu bewerten, was die Branche jeweils macht, was als „good practice“ oder best practice gilt. Die bestehenden Rahmenkonzepte des IDW PS 980, der ISO Norm 19600 und später ISO 37301 oder auch der Leitfaden des amerikanischen Department of Justice (DOJ) sollten hier eine sinnvolle Unterstützung sein.

Mit diesem Buch führen wir durch die bekannten Elemente des CMS und geben Hinweise darüber, wie das System angemessen aufgebaut werden kann und zwar im Hinblick auf eine etwaige Prüfung. Die Autoren sind allesamt seit vielen Jahren in der Compliance Beratung und Prüfung tätig und blicken auf eine Vielzahl an Prüfungen zurück.

Im ersten Teil beleuchten *Jan-Hendrik Gnädiger* und Kollegen den aktuellen Stand und die Entwicklung von Compliance Management in Deutschland in den letzten Jahren. Zudem wird die Prüfung nach IDW PS 980 dargestellt und die Vorgehensweise vom Readiness Check bis hin zur Wirksamkeitsprüfung beschrieben.

Im zweiten Teil führen die Hauptautoren *Verena Brandt*, *Marc Stauder* und *Jan-Hendrik Gnädiger* durch die Elemente des Prüfungsstandards und beschreiben hierzu die Good Practices im Compliance Management sowie die Erfahrungen aus der Praxis.

Der dritte Teil beschäftigt sich mit aktuellen Entwicklungen im Compliance Management. Das Thema e-Crime, welches in viele Compliance Bereiche hineinspielt, wird dabei von *Michael Sauerermann* vorgestellt. *Stefan Otremba* betont in seinem Beitrag die Wichtigkeit der Kultur für das Thema Compliance und die Integration von Compliance und Integrität, welche in vielen Unternehmen zu beobachten ist. Im Kapitel Monitorship gibt *Verena Brandt* Einblicke in die Herausforderungen welche Unternehmen im Rahmen eines US Monitorship begegnen und geht hierbei auf die aktuellen Entwicklung in der US-Gesetzgebung ein, welche sich durch den aktuellen Leitfaden des DOJ ergeben haben. *Jan-Hendrik Gnädiger* gibt im Kapitel zum ISO 37001 Standard Einblicke in die ISO-Prüfung eines Anti-Korruption Managements und einen Ausblick auf den neuen ISO 37301 zur Zertifizierung von CMS.

Der vierte Teil des Buchs beschäftigt sich mit der erfolgreichen Integration weiterer Rechtsgebiete in das CMS nach der Prägung des IDW PS 980. Das Augenmerk liegt hierbei auf neuen Entwicklungen und neuen Themen für das Compliance Management. Aus diesem Grund beschreibt *Barbara Scheben* zunächst den Aufbau eines Datenschutz Managementsystem unter den Anforderungen der EU-DSGVO, wie sie seit Mai 2018 für Unternehmen, welche Daten in der EU bzw. von in der EU Ansässigen verarbeiten, gilt. In einem weiteren Kapitel geht sie dann auf das Thema Geldwäsche und die Umsetzung im CMS ein. Im Kapitel Tax Compliance veranschaulicht *Marc Stauder* die Integration von steuerrechtlichen Anforderungen in ein Compliance Management, wie dies inzwischen von den Verwaltungsbehörden gefordert und von den Unternehmen nachzuweisen ist. Im Anschluss wirft *Verena Brandt* mit Kollegen ein neues Licht auf das bekannte Thema Kartellrecht und stellt dies insbesondere in Bezug zu den aktuellen Entwicklungen des VerSanG-E. *Christian Hell* beschreibt die neuen Anforderungen an die Unternehmen hinsichtlich der CSR-Berichtspflichten, wie sie sich aus dem CSR-Richtlinienumsetzungsgesetz ergeben, und wie diese im Rahmen des Compliance Managements betrachtet werden können. Der Abschnitt IT-Compliance von *Guido Havers* und Kollegen beschäftigt sich mit den regulatorischen Anforderungen an die IT und wie diesen i. S. einer IT-Compliance organisatorisch und prozessual begegnet werden kann. *Gerd Krause* gibt Einblicke in eines der neuen Themenfelder im Compliance Management und beschäftigt sich im Kapitel Technical Compliance mit der Thematik, wie technische Anforderungen im Rahmen eines CMS betrachtet und wie Ansätze des Qualitätsmanagements damit verknüpft werden können. Im letzten Kapitel des Buchs wird ebenfalls durch *Gerd Krause* das Teilgebiet des Arbeitsschutzes betrachtet, welcher insbesondere durch die Entwicklungen im Rahmen der Corona-Pandemie noch weiter an Bedeutung gewonnen hat.

Ich danke den Autoren für ihre Arbeit an diesem Buch und wünsche allen Lesern einige neue Erkenntnisse beim Lesen und Erfolg bei der praktischen Umsetzung.

Köln, im August 2020

WP/StB Dipl.-Kfm. Dr. Jan-Hendrik Gnädiger

AUTORENVERZEICHNIS

WP/StB Verena Brandt

Claudia Dietrich

WP/StB Dr. Jan-Hendrik Gnädiger

WP Guido Havers

Christian Hell

Yann Paul Hengstenberg

Timo Herold

Maximilian Kirch

Katharina Kleff

Gerd Krause

Dr. Stefan Otremba

StB Julia Quade

RA Dr. Gerrit Rixen

Max Fabian Röhner

Carolin Sander

Michael Sauermann

RAin Barbara Scheben

Florentin Schlegel

RA Dr. Hannes Schwinn, Lic. en Droit (Lyon III)

WP/StB Marc Stauder

RA Timo Wiesch

INHALTSVERZEICHNIS

Grußwort	V
Autorenverzeichnis	VII
Abbildungsverzeichnis	XVII
Tabellenverzeichnis	XIX
Abkürzungsverzeichnis	XXI

I. Quo Vadis CMS **1**

1.	Aktueller Stand Compliance Management Systeme in Deutschland	1
2.	Was sind Readiness Check und Wirksamkeitsprüfung?	7
2.1	Von der Prüfungsvorbereitung zum Readiness Check	7
2.1.1	Definition der zu prüfenden Teilrechtsgebiete	8
2.1.2	Regionale Abgrenzung	8
2.1.3	Auswahl des Prüfungstyps	8
2.1.4	Bestandsaufnahmen bestehender Compliance-Komponenten	9
2.1.5	Erstellen einer CMS-Beschreibung	9
2.1.6	Durchführung eines Readiness Checks	10
2.2	Von der Prüfbereitschaft zur Wirksamkeitsbescheinigung	10
2.2.1	Die drei Prüfungstypen nach IDW PS 980	11
2.2.2	Die Phasen der Wirksamkeitsprüfung	12
2.2.2.1	Prüfungsplanung	14
2.2.2.2	Prüfungsdurchführung	16
2.2.2.3	Berichterstattung	18
2.3	Mehrjähriger Prüfplan	19

II. Elemente eines wirksamen Compliance Management Systems **21**

1.	Compliance Kultur	22
1.1	Subelemente	23
1.1.1	Personalpolitik	23
1.1.2	Top Management Commitment	24
1.1.3	Führungsstil	25
1.1.4	Sanktionierung	26
1.1.5	Anreizsysteme	27
1.1.6	Unternehmenskultur	28
1.1.7	Aufsichtsorgan	28
1.2	Erfahrungen und Erkenntnisse aus der Praxis	29

2.	Compliance Ziele	31
2.1	Positionierung	31
2.2	Vorgehensweise der Zielsetzung	32
2.2.1	Zielbildung	33
2.2.2	Planung	33
2.2.2.1	Messbarkeit des Grads der Zielerreichung	33
2.2.2.2	Abstimmung der Verfügbarkeit der Ressourcen	34
2.2.3	Ausführung	34
2.2.4	Kontrolle	34
2.3	Definition der Ziele	34
2.3.1	Abgrenzung relevanter Teilbereiche für das CMS	34
2.3.2	Risikominderung	35
2.3.3	Effizienz- und Effektivitätssteigerung	37
2.3.4	Transparenz	37
2.4	Geltungsbereich	38
2.5	Erfahrungen und Erkenntnisse aus der Praxis	38
3.	Compliance Risiken	40
3.1	Risiko-Relevanz-Analyse	40
3.2	Compliance Risk Assessment	41
3.2.1	Top-Down Risk Assessment	41
3.2.2	Bottom-Up Risk Assessment	42
3.3	Integration in das unternehmensweite Risikomanagement	44
3.3.1	Risikomanagement System	44
3.3.2	Internes Kontrollsystem	45
3.4	Erfahrungen und Erkenntnisse aus der Praxis	47
4.	Compliance Programm	49
4.1	Regelungsarten und Regelungsprozesse	49
4.2	Umsetzung von unternehmensinternen Regelungen	51
4.2.1	Gesellschaftsrechtliche Umsetzung	52
4.2.2	Arbeitsrechtliche Umsetzung	52
4.2.3	Datenschutzrechtliche Aspekte und ihre Außenwirkung	53
4.3	Außenwirkung von Regelungen	54
4.4	Maßnahmen zur Begrenzung von Compliance Risiken	55
4.4.1	Compliance Kontrollen	55
4.4.2	Maßnahmen zur Aufdeckung	55
4.4.3	Geschäftspartner-Due-Diligence	56
4.4.4	Einbeziehung von Integritätsklauseln in die Vertragsgestaltung	58
4.4.5	Compliance Schulungen	59
4.4.6	Hinweisgebersysteme	59
4.5	Erfahrungen und Erkenntnisse aus der Praxis	62

5.	Compliance Organisation	64
5.1	Delegation	64
5.1.1	Horizontale Delegation	64
5.1.2	Vertikale Delegation	65
5.1.3	Kontrollpflichten des Vorstands	65
5.1.4	Delegationsschreiben	65
5.2	Verortung der Compliance Organisation	65
5.3	Ausgestaltung der Compliance Organisation	68
5.3.1	Chief Compliance Officer	68
5.3.2	Compliance Committee	70
5.3.3	Ombudssystem	71
5.3.4	Berichtswege	71
5.4	Ressourcenausstattungen	72
5.5	Erfahrungen und Erkenntnisse aus der Praxis	72
6.	Compliance Kommunikation	74
6.1	Nachhaltigkeit des Kommunikationskonzepts	74
6.2	Wissensaufbau zu Compliance	75
6.2.1	Schulungsmaßnahmen	76
6.2.2	Ergänzende Kommunikationsinstrumente	79
6.3	Interne Berichtspflichten und Berichtswege	81
6.3.1	Berichte über Hinweise	81
6.3.2	Kommunikation an die Unternehmensführung	82
6.3.3	Kommunikation mit dem Aufsichtsrat	83
6.3.4	Kommunikation mit anderen Bereichen	83
6.4	Externe Compliance und Krisenkommunikation	83
6.5	Erfahrungen und Erkenntnisse aus der Praxis	85
7.	Überwachung und Verbesserung des CMS	87
7.1	Dokumentationserfordernis	88
7.2	Überwachungsmaßnahmen	88
7.2.1	Prozessintegrierte Überwachung	88
7.2.2	Prozessunabhängige Überwachung	89
7.2.3	Self-Assessments	91
7.2.4	Überwachung der Compliance Kultur	91
7.2.5	Überwachung der Rahmenbedingungen	92
7.3	Reaktion auf Schwachstellen und Verstöße	93
7.3.1	Reaktion auf Verstöße	93
7.3.2	Reaktion auf festgestellte Schwächen des CMS	94
7.4	Unterschied zwischen systemimmanenter Überwachung und externer Prüfung	94
7.5	Erfahrungen und Erkenntnisse aus der Praxis	95

III. Aktuelle Themen im Compliance Management	97
1. E-Crime	97
1.1 Einleitung	97
1.2 Die relevanten Delikte	97
1.3 Die Täter	99
1.4 Die Schäden	99
1.5 Aktuelle Entwicklung der Computerkriminalität	100
1.5.1 Aktuelle Trends	101
1.5.1.1 Ransomware	101
1.5.1.2 Schwachstelle Mensch – Sicherheitslücken durch Social Engineering	102
1.5.1.3 Identitätsdiebstahl/Phishing	103
1.6 Prävention, Detektion und Reaktion	104
1.6.1 Faktor Personal	104
1.6.2 Investitionen	104
1.6.3 Security Operations Center (SOC)/Computer Emergency Response Team (CERT)	105
1.6.4 Cyber-Versicherungen	105
1.7 Ausblick	106
2. Die Unternehmenskultur als Nexus eines nachhaltigen Compliance Managements	107
2.1 Der Ausgangspunkt: Steigende normative Anforderungen	107
2.2 Die „klassische“ Antwort: Regel- und kontrollbasiertes Compliance Management	108
2.3 Die „moderne“ Antwort: Kulturbasiertes Compliance Management	108
2.4 Das Zielbild: Orientierung in der VUKA-Welt	111
3. Monitorship	113
3.1 Einleitung	113
3.2 Grundlagen und Rahmenbedingungen für ein Monitorship	113
3.2.1 Die Rolle des Monitors	113
3.2.2 Auslöser für Monitorships	115
3.2.3 Auswahl eines Monitors	115
3.2.4 Rechtliche Grundlagen	116
3.2.4.1 Rahmenbedingungen für U.S. Monitorships	116
3.2.4.2 Impulse durch das Verbandssanktionengesetz	117
3.2.5 Ablauf eines Monitorships	119
3.3 Monitorships in der Praxis	120
3.3.1 Aktuelle Monitorverfahren im Überblick	120
3.3.2 Wichtige Erfolgsfaktoren für ein Monitorship	121
3.3.2.1 Strategie und Zielbild	121
3.3.2.2 Projektorganisation und Projektmanagement	124
3.3.2.3 Berichte und Empfehlungen des Monitors	125

3.3.2.4	Zusammenarbeit mit dem Monitor	125
3.3.2.5	Rolle der Internen Revision	126
3.4	Ausblick	126
4.	ISO 37001 – Hintergrund und Anwendungsmöglichkeiten	128
4.1	Hintergrund und Entwicklung	128
4.2	ISO 37001 und IDW PS 980	129
4.3	Kernaspekte im Zertifizierungsprozess	131
4.4	Der Weg zur Zertifizierung	132
4.4.1	Risikobewertung und Scoping	132
4.4.2	Audit Stufe 1	133
4.4.3	Audit Stufe 2	133
4.4.4	Überwachungsaudits und Rezertifizierung	134
4.5	Nutzen einer Zertifizierung nach ISO 37001	134
4.5.1	Nutzen im Umgang mit Geschäftspartnern und Behörden	134
4.5.2	Unternehmensbezogener Nutzen	135
4.6	Möglichkeit zur Nutzung im Rahmen der Lieferketten-Compliance	135

IV. Erfolgreiche Integration ausgewählter Teilrechtsgebiete in das CMS **137**

1.	Datenschutz-Management-Systeme	137
1.1	Herausforderungen	137
1.1.1	Die Grundsätze der Verarbeitung personenbezogener Daten nach der DSGVO	138
1.1.2	Ausgewählte Pflichten des Verantwortlichen	139
1.1.3	Die Rechenschaftspflicht des Verantwortlichen	140
1.1.4	Die Verantwortlichkeit für die Umsetzung der DSGVO-Vorgaben	140
1.1.5	Die Notwendigkeit eines Datenschutz-Management-Systems	141
1.2	Aktuell diskutierte Lösungsansätze	142
1.3	Handlungsempfehlungen	143
1.4	Ausgewählte branchen- und segmentspezifische Besonderheiten	148
1.5	Fazit	149
2.	Das geldwäschebezogene Risikomanagement	150
2.1	Der Anwendungsbereich des GwG	150
2.2	Risikomanagement	151
2.2.1	Risikoanalyse	153
2.2.2	Interne Sicherungsmaßnahmen	154
2.2.2.1	Kundenbezogene Sorgfaltspflichten	155
2.2.2.2	Weitere interne Sicherungsmaßnahmen	161
2.3	Transparenzregister	164
2.4	Folgen von Verstößen	165

2.5	Aktuell diskutierte Lösungsansätze	166
2.6	Handlungsempfehlungen	169
2.6.1	Feststellung des Verpflichtetenstatus und Identifizierung möglicher Privilegierungen	169
2.6.2	Umsetzung von Maßnahmen	170
2.6.2.1	Nutzen bereits vorhandener Strukturen	170
2.6.2.2	Orientierung an anerkannten Standards	170
3.	Tax Compliance	173
3.1	Einleitung	173
3.2	Begriffliche und rechtliche Grundlagen der Tax Compliance	174
3.2.1	Definition Tax CMS	174
3.2.2	AEAO zu § 153	175
3.2.3	Abgrenzung § 153 AO zu § 371 AO	176
3.3	Ausgestaltung eines Tax CMS	177
3.3.1	Verantwortlichkeit für die Einrichtung eines Tax CMS	177
3.3.2	Geltungsbereich eines Tax CMS	177
3.3.3	Grundelemente eines Tax CMS	178
3.3.3.1	Tax Compliance Kultur	179
3.3.3.2	Tax Compliance Ziele	180
3.3.3.3	Tax Compliance Risiken	180
3.3.3.4	Tax Compliance Programm	181
3.3.3.5	Tax Compliance Organisation	182
3.3.3.6	Tax Compliance Kommunikation	183
3.3.3.7	Tax Compliance Überwachung und Verbesserung	184
3.4	Prüfung eines Tax CMS	184
3.4.1	Prüfungsziel und Prüfungsgegenstand	184
3.4.2	Prüfungsumfang	185
3.4.3	Berichterstattung und Weitergabe von Prüfungsergebnissen	186
3.5	Trends und Ausblick	186
4.	Kartellrechts-Compliance	189
4.1	Einleitung	189
4.2	Kartellrecht – Rechtliche und praktische Grundlagen	189
4.2.1	Grundlagen des EU- und deutschen Kartellrechts, insbesondere Kartellverbot	189
4.2.2	Wesentliche Teilbereiche des EU- und deutschen Kartellrechts	191
4.2.2.1	Horizontale Wettbewerbsbeschränkungen	191
4.2.2.2	Austausch wettbewerbsch sensibler Informationen zwischen Wettbewerbern	191
4.2.2.3	Vertikal bewirkte Wettbewerbsbeschränkungen	192

4.2.2.4	Missbrauch einer marktbeherrschenden Stellung	192
4.2.2.5	Fusionskontrolle	193
4.2.3	Wesentliche Rechtsfolgen	194
4.3	Berücksichtigung unternehmensbezogener Risiken und Umfeldfaktoren für ein kartellrechtliches CMS	195
4.3.1	Risikobasierter Ansatz und Scoping	195
4.3.2	Kartellrechtliche Umfeldfaktoren und branchenspezifische Besonderheiten	196
4.4	Handlungsempfehlungen und Best-Practices	196
4.4.1	Compliance Kultur	197
4.4.2	Compliance Ziele	198
4.4.3	Compliance Risiken	198
4.4.4	Compliance Organisation	199
4.4.5	Compliance Programm	199
4.4.6	Compliance Kommunikation	201
4.4.7	Compliance Überwachung & Verbesserung	201
4.5	Aktuelle Entwicklungen und Herausforderungen für kartellrechtliche CMS	202
4.5.1	Digitalisierung	202
4.5.2	Verbandssanktionengesetz	202
5.	Integration von Themen der Nachhaltigkeit über die CSR-Berichtspflicht in das CMS (Beispiel Menschenrechte)	204
5.1	Herausforderungen	207
5.2	Aktuell diskutierte Lösungsansätze	208
5.3	Handlungsempfehlungen	211
5.4	Ausgewählte branchen- und segmentspezifische Besonderheiten	211
6.	IT-Compliance	212
6.1	Herausforderungen	213
6.1.1	Unternehmensspezifische Zieldefinition	213
6.1.2	Unternehmensspezifisches IT-Regelwerk und Regelungsambivalenz	213
6.1.3	Verantwortungsvoller Umgang mit IT und Informationen	215
6.1.4	Wirtschaftskriminalität	216
6.1.5	Datenschutz, Informationssicherheit und Geschäftsgeheimnisschutz	217
6.2	Aktuell diskutierte Lösungsansätze	218
6.2.1	Das „Three Lines of Defense“-Modell als organisatorischer Lösungsrahmen	218
6.2.2	IT-Strukturanalyse und Schutzbedarfsfeststellung als Lösungsrahmen für IT-Sicherheit	219
6.2.3	IT-Investmentportfolio-Analyse als Lösungsrahmen für anwendungsbezogene Risiken	220
6.3	Handlungsempfehlungen auf Basis des IDW PS 980	222

6.4	Ausgewählte branchen- und segmentspezifische Besonderheiten in kritischen Infrastrukturen	224
6.5	Abschließende Betrachtung der IT-Compliance	224
7.	Technische Compliance – Compliance in der Produktentwicklung und Produktion	225
7.1	Einführung in das Teilrechtsgebiet	225
7.2	Grundelemente eines CMS im Teilrechtsgebiet	227
7.2.1	Compliance Kultur	228
7.2.2	Compliance Ziele	228
7.2.3	Compliance Risiken	230
7.2.4	Compliance Programm	231
7.2.5	Compliance Organisation	233
7.2.6	Compliance Kommunikation und Information	234
7.2.7	Compliance Überwachung und Verbesserung	235
7.3	Praxishinweise zur Integration des Teilrechtsgebiets in das CMS	236
7.3.1	Compliance Ziele	236
7.3.2	Risikoanalyse	236
7.3.3	Umsetzung des „3-Lines-of-Defense“-Modells	237
7.3.4	Einsatz von Software	237
8.	Compliance in Arbeitssicherheit und Gesundheitsschutz	238
8.1	Einführung in das Teilrechtsgebiet	238
8.2	Grundelemente eines CMS im Teilrechtsgebiet	239
8.2.1	Compliance Kultur	240
8.2.2	Compliance Ziele	241
8.2.3	Compliance Risiken	243
8.2.4	Compliance Programm	245
8.2.5	Compliance Organisation	247
8.2.6	Compliance Kommunikation und Information	248
8.2.7	Compliance Überwachung und Verbesserung	249
8.3	Praxishinweise zur Integration des Teilrechtsgebiets in das CMS	250
8.3.1	Compliance Ziele	250
8.3.2	Risikoanalyse	250
V.	Fazit und Ausblick	252
	Literaturverzeichnis	253
	Stichwortverzeichnis	263

ABBILDUNGSVERZEICHNIS

ABB. 1:	Die Phasen der Wirksamkeitsprüfung	13
ABB. 2:	Der Weg der CMS-Beschreibung zum Prüfprogramm	16
ABB. 3:	Systematisierung der Prüfungshandlungen eines CMS-Prüfers	17
ABB. 4:	Die Prüfungsziele auf Aussageebene	18
ABB. 5:	Fragestellungen bei der Prüfungsdurchführung	18
ABB. 6:	Idealtypischer Verlauf einer CMS-Prüfung	20
ABB. 7:	Subelemente der Compliance Kultur	23
ABB. 8:	Tone from the Top	25
ABB. 9:	Hierarchie der Compliance Ziele	32
ABB. 10:	Teilaufgabe der Compliance Ziele	32
ABB. 11:	Ziele	37
ABB. 12:	Geltungsbereich	38
ABB. 13:	Integration	43
ABB. 14:	Zusammenspiel der Governance-Elemente	44
ABB. 15:	COSO-Würfel	45
ABB. 16:	Regelungsbereich des IKS	46
ABB. 17:	Schritte zu einem erfolgreichen Compliance Verständnis	51
ABB. 18:	Hybride Organisationsstrukturen	66
ABB. 19:	Stellung der Compliance Organisation im Unternehmen	71
ABB. 20:	Prozess zur Ermittlung des Personalbedarfs	72
ABB. 21:	Dimensionen der Unternehmenskultur	109
ABB. 22:	High-Level-Structure der ISO 37001	129
ABB. 23:	IDW PS 980 und ISO 37001	130
ABB. 24:	Prozestufen der Zertifizierung nach ISO 37001	132
ABB. 25:	Elemente und Ausnahmetatbestände des Risikomanagements	152
ABB. 26:	Elemente des Risikomanagements und interner Sicherungsmaßnahmen	154
ABB. 27:	Übersicht der allgemeinen Kundensorgfaltspflichten	157
ABB. 28:	Übersicht der vereinfachten Kundensorgfaltspflichten	158
ABB. 29:	Übersicht der verstärkten Kundensorgfaltspflichten	159
ABB. 30:	Sieben Grundelemente des Tax CMS	179
ABB. 31:	Die Säulen des Kartellrechts	191
ABB. 32:	Design eines Social Compliance Management Systems	210
ABB. 33:	Modell der „Datenpyramide“	215
ABB. 34:	Three Lines of Defense	219
ABB. 35:	IT Investitionsportfolio	221

TABELLENVERZEICHNIS

TAB. 1:	Grundelement und Subelemente für das Grundelement Kultur	15
TAB. 2:	Risiken - Warum aktiv Menschenrechte adressieren?	208
TAB. 3:	Heat Map	221
TAB. 4:	Ausgewählte Strukturdaten zu Produkten und Dienstleistungen	226
TAB. 5:	Beispielhafte Auswahl von relevanten Produktrückrufen, Bußgeldern und Strafen	226
TAB. 6:	Gegenüberstellung relevanter Standards	227
TAB. 7:	Beispiele technischer Anforderungen als Grundlage für die Setzung von Compliance Zielen	230
TAB. 8:	Beispiel für die Bildung von Risikoträgern durch Kombination verschiedener Merkmale	231
TAB. 9:	Beispiele für Anforderungen an operative Kernprozesse mit wesentlichen Kontrollen	232
TAB. 10:	Typische Funktionen im „3 Lines of Defense“-Modell	234
TAB. 11:	Auswahl von Praxisbeispielen	237
TAB. 12:	Ausgewählte Strukturdaten zur Erwerbstätigkeit in Deutschland	239
TAB. 13:	Beispielhafte Auswahl von relevanten Regressnahmen, Bußgeldern und Strafen	239
TAB. 14:	Gegenüberstellung relevanter Standards	240
TAB. 15:	Beispiele technischer Anforderungen als Grundlage für die Setzung von Compliance Zielen	242
TAB. 16:	Beispiel für die Verknüpfung von technischen Anforderungen mit Gefährdungs- und Belastungsfaktoren der Arbeitshilfe BG RCI A017	244
TAB. 17:	Beispiele für Kontrollen	246
TAB. 18:	Typische Funktionen im „3 Lines of Defense“-Modell	248
TAB. 19:	Auswahl von Praxisbeispielen	251

ABKÜRZUNGSVERZEICHNIS

A

a. F.	alte Fassung
AaaS	Attack-as-a-Service
AG	Aktiengesellschaft
ASiG	Arbeitssicherheitsgesetz

B

BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BB	Zeitschrift Betriebs-Berater
BCM	Business Continuity Management
BDSG	Bundesdatenschutzgesetz
BKA	Bundeskriminalamt
BMJV	Bundesministerium der Justiz und für Verbraucherschutz
BNP	Banque Nationale de Paris
BSI	Bundesamt für Sicherheit in der Informationstechnik
bspw.	beispielsweise

C

CB	Zeitschrift Compliance Berater
CCO	Chief Compliance Officer
CCZ	Corporate Compliance Zeitschrift
CERT	Computer Emergency Response Team
CMS	Compliance Management System
COSO	Commission of Sponsoring Organizations of the Treadway Commission
CPI	Corruption Perception Index
CRA	Compliance Risk Assessment

D

DB	Zeitschrift – Der Betrieb
DCGK	Deutscher Corporate Governance Kodex
DFSS	Design for Six Sigma
DGUV	Deutsche Gesetzliche Unfallversicherung
DICO	Deutsches Institut für Compliance e.V.
DOJ	Department of Justice
DoS	Denial of Service
DSGVO	Datenschutz-Grundverordnung (VO EU 2016/679)

DSMS	Datenschutz-Management-System
DStR	Zeitschrift Deutsches Steuerrecht

E

ECI	Ethics and Compliance Initiative
EU	Europäische Union
EWR	Europäischer Wirtschaftsraum

F

FCA	Financial Conduct Authority
FCPA	Foreign Corrupt Practices Act
FIU	Financial Intelligence Unit
FKVO	Fusionskontrollverordnung

G

GeschGehG	Gesetz zum Schutz von Geschäftsgeheimnissen
ggf.	gegebenenfalls
GmbHR	Zeitschrift GmbH-Rundschau
GRC	Corporate Governance, Risk Management und Compliance Management
GrCh	Charta der Grundrechte der Europäischen Union
GwG	Geldwäschegesetz

H

HSBC	Hongkong and Shanghai Banking Corporation
------	---

I

i. d. R.	in der Regel
i. H.	in Höhe
IBRD	International Bank for Reconstruction and Development
ICC	Internationale Handelskammer
IDA	International Development Association
IDW	Institut der Wirtschaftsprüfer in Deutschland
IKS	internes Kontrollsystem
IoT	Internet of Things
ISO	International Organization for Standardization
IT	Informationstechnologie

K

KI	Künstliche Intelligenz
KYC	Know-Your-Customer

M

M&A	Mergers & Acquisitions
-----	------------------------

N

NAP	Nationalen Aktionsplan für Wirtschaft und Menschenrechte
NZA	Neue Zeitschrift für Arbeitsrecht
NZG	Neue Zeitschrift für Gesellschaftsrecht

O

o. g.	oben genannt(e)
o. O.	ohne Ort/ohne Ortsangabe
o. S.	ohne Seitenangabe
OCEG	Open Compliance and Ethics Group
OFAC	U.S. Department of the Treasury's Office of Foreign Assets Control
OWiG	Gesetz über Ordnungswidrigkeiten

P

PEP	politisch exponierte Person
PKS	Polizeiliche Kriminalstatistik
ProdSG	Produktsicherheitsgesetz

R

RL	Richtlinie
RMS	Risikomanagement System
RPA	Robotic Process Automation

S

SCP	Compliance Sanctions Program
SDG	UN Sustainable Development Goals
SEC	Securities and Exchange Commission
SoC	Social Compliance
SOX	Sarbanes-Oxley Act
SteuK	Zeitschrift Steuerrecht kurzgefaßt

T

TKG	Telekommunikationsgesetz
TQM	Total Quality Management

U

u.U.	unter Umständen
Ubg	Zeitschrift – Die Unternehmensbesteuerung
UNCAC	UN Convention against Corruption
UTM	Unified Threat Management
UWG	Gesetz gegen den unlauteren Wettbewerb

V

VerSanG-E	Referentenentwurf Verbandssanktionengesetz
VO	Verordnung
VUKA	Volatilität, Unsicherheit, Komplexität und Ambiguität

W

WpDVerOV	Verordnung zur Konkretisierung der Verhaltensregeln und Organisationsanforderungen für Wertpapierdienstleistungsunternehmen
WpHG	Wertpapierhandelsgesetz

Z

z. B.	zum Beispiel
ZD	Zeitschrift für Datenschutz
ZGR	Zeitschrift für Unternehmens- und Gesellschaftsrecht
ZHR	Zeitschrift für das gesamte Handelsrecht und Wirtschaftsrecht
ZIP	Zeitschrift für Wirtschaftsrecht
ZRFC	Zeitschrift Risk, Fraud & Compliance
ZWH	Zeitschrift Wirtschaftsstrafrecht und Haftung im Unternehmen

I. Quo Vadis CMS

1. Aktueller Stand Compliance Management Systeme in Deutschland

WP/StB Dr. Jan-Hendrik Gnädiger und Timo Herold

In den 1980er Jahren häuften sich Fälle von Korruption und Insiderhandel in der amerikanischen Finanzbranche und da in dem Zusammenhang verhängte Bußgelder und Geldstrafen nicht die gewünschten Verhaltensänderungen bewirkten, wurden neue Wege beschritten. So ermöglichten die 1991 überarbeiteten *U.S. Federal Sentencing Guidelines* explizit ein vermindertes Strafmaß, für den Fall, dass beklagte Unternehmen interne Regelungen zur Prävention von Gesetzesverstößen implementieren, kommunizieren und überwachen.¹ Dadurch wurde der Grundstein für das Compliance Management System (CMS) gelegt.

Der aus dem angelsächsischen Sprachgebrauch übernommene Begriff Compliance stammt ursprünglich aus dem medizinischen Bereich. Eine gesetzliche Definition des Compliance-Begriffs hat in Deutschland bisher nicht stattgefunden und ist durch die Unterschiede des deutschen Rechtssystems zum amerikanischen, welchem die Unternehmenshaftung zugrunde liegt, auch nur eingeschränkt übertragbar.² Im betriebswirtschaftlichen und rechtswissenschaftlichen Kontext steht Compliance für die Regeltreue von Unternehmen und somit für die Einhaltung von Gesetzen, Richtlinien und freiwilligen Kodizes.³ Der Deutsche Corporate Governance Kodex (DCGK) definiert Compliance als die in der Verantwortung des Vorstands liegende Einhaltung der gesetzlichen Bestimmungen und unternehmensinternen Richtlinien.⁴ In manchem Unternehmen wird die Definition um die „freiwillige Selbstverpflichtung“ ergänzt. Demzufolge ist das Compliance Management die Summe an Maßnahmen, welche dazu dienen, die auf Basis einer Risikoanalyse als notwendig identifizierte Regeleinhaltung (Compliance) sicherzustellen. Im Sinne eines angemessen eingerichteten und wirksamen CMS geht es auch darum, die Organisation und entsprechende Maßnahmen nachweisbar vorzuhalten.⁵

In den 1990er Jahren und zu Beginn der 2000er Jahre wurde das Compliance Management auch in Deutschland in Unternehmen eingeführt, jedoch blieb das systematische Betreiben eines CMS beschränkt auf wenige große oder durch spezialgesetzliche Vorschriften regulierte Unternehmen, wie bspw. in der Finanzbranche. Bei den Großunternehmen wurde dies maßgeblich durch ihre internationale Tätigkeit und den Bezug durch die USA getrieben.⁶ Auch thematisch war der Begriff Compliance eingeschränkt auf die Rechtgebiete Anti-Korruption, Kartellrecht und in der Finanzbranche auch Insiderhandel und Geldwäsche. Eine flächendeckende Imple-

1 Vgl. Geißler, Harvard Business Manager 2/2004 S. 17.

2 Vgl. Mittendorf, Compliance Management System als Haftungsbegrenzungsinstrument in der mittelständischen Wirtschaft, Berlin 2017, Rz. 5–28 (5).

3 Vgl. Hauschka/Moosmayer/Lösler, 1. Einführung, in: Hauschka/Moosmayer/Lösler (Hrsg.), Corporate Compliance: Handbuch zur Haftungsvermeidung im Unternehmen, 3. Aufl. 2016, Rz. 1–85 (2).

4 Vgl. BMJV, Bekanntmachung des Deutschen Corporate Governance Kodex in der Fassung v. 24.6.2014 (BAnz AT 30.9.2014 B1, 4.1.3).

5 Vgl. United States Sentencing Commission, 2018 Guidelines Manual, § 8 B 2.1., S. 517 ff.

6 Vgl. Labinsky, Environmental Compliance: Eine rechtsvergleichende Untersuchung der Unternehmensorganisationspflichten in den USA und Deutschland mit Fokus auf dem Umweltrecht, 2019, S. 39.

mentierungswelle wurde gegen Ende der 2000er Jahre durch mehrere Unternehmensskandale ausgelöst. Inzwischen wurden entsprechende Systeme in fast allen deutschen Großunternehmen und in großen Teilen des Mittelstands eingeführt.⁷

Dies wurde begleitet durch die Entwicklung und Veröffentlichung entsprechender Rahmenwerke für die Prüfung bzw. Zertifizierung von CMS oder als Praxisleitfaden für die Implementierung. Im Jahr 2011 veröffentlichte das Institut der Wirtschaftsprüfer in Deutschland (IDW) mit dem Prüfungsstandard 980 (IDW PS 980) „Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen“ ein Rahmenwerk für die Prüfung von CMS.⁸ Dieses Rahmenwerk ist mit seinen sieben Grundelementen in Deutschland nach wie vor die Basis für Compliance Management. Im gleichen Jahr veröffentlichte der TÜV Rheinland mit dem TR CMS 101:2011 „Standard für Compliance Management Systeme“ ebenfalls ein Rahmenwerk für die Prüfung bzw. Zertifizierung. Dieser wurde 2015 durch eine neue Fassung „Standard für Compliance-Management-Systeme“ (TR CMS 101:2015) abgelöst und um den Compliance-Leitfaden (TR CMS 100:2015) ergänzt.⁹

Auch auf internationaler Ebene wurde durch die Internationale Organisation für Normung (ISO) im Jahr 2014 ein Standard mit Empfehlungen und Umsetzungsbeispielen veröffentlicht. Der ISO 19600:2014 „Compliance Management Systeme“ stellt dabei eine Grundnorm für CMS dar und basiert auf Vorläufern aus Australien und Österreich.¹⁰ Beim ISO 19600 handelt es sich um einen Einrichtungsstandard, bei dem kein Zertifikat ausgestellt wird. Eine Bescheinigung über die Einhaltung der aufgeführten Leitlinien lässt sich aber bspw. im Rahmen einer IDW PS 980 Prüfung oder nach ISAE 3000 (International Standard on Assurance Engagements von der International Federation of Accountants (IFAC)) erteilen. Mit dem ISO 37001:2016 „Anti-bribery management systems“ wurde durch die ISO ein weiterer Standard für das Spezialgebiet Anti-Korruption veröffentlicht. Dieser wird insbesondere von international tätigen Unternehmen dafür genutzt ihr Anti-Korruptions-Managementsystem zu implementieren und zunehmend auch danach zu zertifizieren. Für 2021 ist mit dem ISO 37301 die Zertifizierung des gesamten CMS nach ISO Standard voraussichtlich möglich. Und der am 21.4.2020 durch das Bundesministerium der Justiz und für Verbraucherschutz (BMJV) veröffentlichte Referentenentwurf zum viel diskutierten sog. Verbandssanktionengesetz (Gesetz zur Stärkung der Integrität in der Wirtschaft, VerSanG-E) bringt eine weitere Dynamik in das Thema.

Allerdings sind CMS in deutschen Unternehmen nicht mehr auf das Thema Anti-Korruption beschränkt. Durch die zunehmende Regulierung und die Forderung nach entsprechenden Systemen rücken stetig weitere Rechtsgebiete bei den Unternehmen in den Fokus. Im Anwendungserlass (AEAO) zu § 153 AO im Jahr 2016 hat das Bundesministerium der Finanzen zur Abgrenzung von Berichtigungs- und Selbstanzeigen Stellung genommen und hier verlautbart, dass wenn der Steuerpflichtige ein innerbetriebliches Kontrollsystem eingerichtet hat, dies gegen das Vorliegen eines Vorsatzes oder der Leichtfertigkeit sprechen kann. Das innerbetriebliche Kontrollsystem kann somit als Teilbereich eines CMS, welches grundsätzlich auf die Einhaltung steuerlicher Vorschriften gerichtet ist (Tax CMS) angesehen werden, welches bei Vorliegen ent-

7 Vgl. *Bussmann/Salvenmoser/Ieker*, CCZ 5/2016 S. 235–240.

8 Vgl. IDW PS 980, WPg Supplement 2/2011 S. 78 ff., FN-IDW 4/2011, S. 203 ff.

9 Vgl. *Schlegel*, Zeitschrift für Fraud, Risk & Compliance 2/2016 S. 55–62.

10 Vgl. *Fissenewert*, Praxishandbuch internationale Compliance-Management-Systeme, 2015, S. 53–54.

haftend wirkt.¹¹ Das IDW hat hierzu im Jahr 2016 einen Praxishinweis „Ausgestaltung und Prüfung eines Tax Compliance Management Systems gemäß IDW PS 980“ veröffentlicht. Aber auch das Thema Geldwäsche ist mit Novellierung des Geldwäschegesetzes (GwG) im Jahr 2017 und damit der Umsetzung der 4. EU-Geldwäscherichtlinie in nationales Recht ein neues Compliance Teilgebiet. Was zuvor nur ein branchenspezifisches Compliance-Gebiet für Unternehmen der Finanzbranche war wurde durch die erweiterte Verpflichtung der sog. Güterhändler zu einem relevanten Teilgebiet für viele Industrie- und Handelsunternehmen.¹² Eine weitere regulatorische Erweiterung des Compliance-Fokus ist in den vergangenen Jahren im Bereich des Datenschutzes zu beobachten. Dies wurde von dem Inkrafttreten der EU Datenschutz-Grundverordnung im Jahr 2018 getrieben. Hierdurch entstanden für die Unternehmen weitere Dokumentations- und insbesondere Rechenschaftspflichten, welche die Handhabung im Rahmen eines CMS notwendig machen.

Weitere regulatorische Treiber können in rechtsgebietsübergreifenden Leitlinien gesehen werden. Am 30.4.2019 hat das Department of Justice (DOJ) Criminal Division seine Richtlinien für Corporate-Compliance-Programme aktualisiert und diese umfassend erweitert. Die aktuellen DOJ-Richtlinien mit dem Titel „Evaluation of Corporate Compliance Programs“ erweitern die vorherige „Compliance Guidance 2017“ um das Doppelte. Darin formuliert das US-Justizministerium seine Erwartungen an die Gestaltung, die Umsetzung und die Wirksamkeit von Compliance Programmen. Hinzugekommen sind insgesamt 61 neue Faktoren, die sich über diese drei großen Themenbereiche erstrecken. Zwar ist die DOJ Guidance kein Gesetz mit unmittelbarer Rechtswirkung, bietet aber den Verfolgungsbehörden in den USA Leitlinien zur Beurteilung, ob Compliance Programme angemessen konzeptioniert und effektiv umgesetzt sind. Sie sollte auch von Nicht-US-Unternehmen für den Auf- und Ausbau ihrer Systeme genutzt werden, da aufgrund der extraterritorialen Wirkung des US-Strafrechts und der verhältnismäßig geringen Anforderungen, die eine Zuständigkeit der US-Verfolgungsbehörden begründen, auch deutsche Unternehmen in den Fokus geraten können. Durch seine Funktion als Bewertungshilfe für die Verfolgungsbehörden bei der Durchführung einer Investigation und bei Sanktionsentscheidungen gibt die DOJ Guidance somit Orientierung, welche Umstände sich schärfend oder mildernd auswirken.¹³

In eine ähnliche Richtung geht auch der Referentenentwurf des BMJV, VerSanG-E. Dieser sieht vor, dass Unternehmen im Falle von Straftaten drastischer und auf andere Art sanktioniert werden, als es bisher nach dem Gesetz über Ordnungswidrigkeiten (OWiG) der Fall war. Gleichzeitig werden Anreize geschaffen, damit Unternehmen kriminelles Verhalten bereits im Vorfeld verhindern und begangene Straftaten selbstständig aufklären. Auf Basis des VerSanG-E soll ein Unternehmen zukünftig für Verbandstaten, welche aus den Unternehmen heraus begangen wurden, sanktioniert werden, sofern es entweder durch die Tat bereichert werden sollte oder eine unternehmensbezogene Pflicht verletzt wurde. Dies kann erfolgen, wenn eine Leitungsperson in die Tat involviert ist oder wenn die Tat durch mangelhafte Aufsicht erleichtert worden ist. Damit stellt das VerSanG-E die bisherige Rechtspraxis in Deutschland auf eine neue Basis. Unternehmen müssen hierauf mit der Einrichtung bzw. Weiterentwicklung entsprechender Systeme rea-

11 Vgl. *Pielke*, Tax Compliance: Effektive Organisation der Einhaltung steuerlicher Pflichten, 2018, S. 5–10.

12 Vgl. *Euskirchen*, Geldwäscheprävention und Compliance Management Systeme, 2017, S. 8–9.

13 Vgl. *Federmann/Gnädiger/Scheben*, Zeitschrift für Fraud, Risk & Compliance 6/2019 S. 268–275.

gieren, denn das Vorliegen eines geeigneten CMS kann bereits dazu führen, dass die Voraussetzungen einer Sanktionierung nicht vorliegen. Sollte eine Verbandssanktion ausgesprochen werden, ist das Vorliegen eines geeigneten CMS maßgeblich für die Art und die Höhe dieser.

Doch nicht nur durch regulatorische Änderungen rücken Themen in den Fokus der öffentlichen Wahrnehmung. In der Automobilindustrie ist, ausgelöst durch den Diesel-Skandal, eine Erweiterung des Compliance Managements durch Produkt bzw. Technische Compliance zu beobachten. Dabei geht es um die organisierte Vermeidung des Inverkehrbringens von nicht sicheren Produkten, die klassische Produkthaftung, bzw. von Produkten, welche nicht den zugesagten Eigenschaften bzw. rechtlichen Vorschriften entsprechen. Dies wurde in der Vergangenheit oftmals im Rahmen des Qualitäts- oder auch des Umweltmanagements gehandhabt; dieses Thema rückt nun als neues Compliance Gebiet in das CMS.

Die Lieferkette wird ein weiterer Aspekt werden. Die Vereinten Nationen und vor allem die westliche Wertegemeinschaft rücken die Einhaltung von Menschenrechten, Umweltschutz und Arbeitssicherheit (Social Compliance) in den Fokus des CMS. Insbesondere aufgrund der Tatsache, dass das Supply Chain Management in einer eigenen Aufbau- und Ablauforganisation organisiert ist, wird die Integration der genannten Anforderungen eine interessante Aufgabe sein. Vereinfacht muss das Unternehmen sicherstellen, dass die Arbeitsteilung entlang der Lieferkette die entsprechenden Vorgaben einhält – das wird im Zuge der anhaltenden Globalisierung und Nutzung immer tiefergehenden Zuliefererpyramiden eine interessante Diskussion werden.

Der Erweiterung des Fokus der CMS durch weitere Rechtsgebiete steht in vielen Unternehmen die Frage nach einer Senkung der Kosten und Erhöhung der Effizienz der Systeme gegenüber. Hier ist das Spannungsfeld zwischen mehr oder gleichbleibender Sicherheit bei gleichzeitiger Reduktion des damit verbundenen Aufwands zu erfüllen, welchem sich viele Compliance Verantwortliche aktuell ausgesetzt sehen. Dies können Unternehmen nur durch die konsequente Integration neuer Themen in bestehende Systeme und durch Digitalisierung dieser erreichen. Neue Rechtsgebiete sollten soweit möglich in die bestehenden Prozesse und Organisation integriert sein. Hierdurch können Abläufe und Methoden sowie hierfür eingesetzte Softwarelösungen mehrfach genutzt werden und es lassen sich dadurch entsprechende Skaleneffekte realisieren. Zudem verhindert dies eine Mehrfachbelastung für die Fachbereiche, denn die wesentlichen Compliance Kosten entstehen oftmals nicht durch die direkten Kosten im Rahmen einer Compliance Organisation sondern durch die indirekten Kosten, welche durch die Teilnahme der Fachbereiche an den Compliance Prozessen entstehen. In einigen Unternehmen lässt sich dies bereits beobachten, bei denen in die bestehenden CMS, die ursprünglich auf Anti-Korruption und Kartellrecht ausgerichtet waren, bereits weitere Rechtsgebiete wie z. B. Datenschutz integriert wurden. In den meisten Unternehmen fand diese Integration bisher nicht statt und die einzelnen Rechtsgebiete werden durch unterschiedliche Bereiche und Silos gesteuert. Die möglichen Synergieeffekte bleiben dadurch ungenutzt.

Zusätzlich besteht für Compliance Verantwortliche die Möglichkeit in die Digitalisierung ihrer Abläufe zu investieren und dadurch die Effizienz zu steigern. Die heutige Technik bietet hierzu unterschiedliche Möglichkeiten. In einem ersten Schritt können hierzu heute manuell durchgeführte Prozesse und Dokumentation in einer digitalen Lösung abgebildet werden. Zudem lassen sich einfache, repetitive Tätigkeiten durch Robotic Process Automation (RPA) entsprechend automatisieren. Dies kann z. B. durch einen einfachen regelbasierten Chat-Bot für einen Compliance Helpdesk realisiert werden. In einer nächsten Ausbaustufe kann dies durch Künstliche In-

telligenz (KI) bzw. Machine Learning noch weiter vorangetrieben werden, so dass auch komplexere Vorgänge durch eine Maschine erledigt werden können. Auch der Einsatz von Data Analytics ist für Compliance Abteilungen denkbar, bspw. wenn es um die Geschäftspartner Due Dilligence geht oder beim Aufdecken von Verstößen. Somit kann nicht nur die Effizienz, sondern auch die Effektivität der Systeme durch den Einsatz von Technologie erhöht werden. Auch hier gibt es einige Unternehmen, die in einzelnen Bereichen bereits in die Digitalisierung ihres CMS investiert haben, jedoch lässt sich auch hier sagen, dass der aktuelle Stand noch hinter den Möglichkeiten zurückbleibt.

Bei all den neuen technischen Möglichkeiten spielt aber weiterhin der Mensch die entscheidende Rolle für das Thema Compliance. Das DOJ betont hierbei insbesondere die Rolle der Kultur für die Wirksamkeit des Compliance Programms. Das Management sollte eine „Kultur der Ethik und Einhaltung der Gesetze“ schaffen und fördern und dies durch das eigene Verhalten demonstrieren. Im Rahmen der Überwachung und Verbesserung sollen die Unternehmen die Compliance Kultur überprüfen und dies über alle Mitarbeitererebenen hinweg. Dies ist in Analogie zum PS 980, in welchem auch die Kultur als die Basis für das CMS definiert ist.¹⁴ Diese Diskussion findet in Deutschland und Europa schon länger statt, aber die Entwicklung ist noch nicht abgeschlossen und die Unternehmen müssen auch in Zukunft noch stärker in die Förderung der Kultur investieren. Dies gelingt nicht durch detailliert ausgearbeitete und digitalisierte Compliance Maßnahmen, sondern durch adressatengerechte Kommunikation und Schulung sowie die Einbindung von Compliance in die operativen Geschäftsprozesse im Unternehmen. Dies kann wiederum durch den Einsatz geeigneter Technologie erreicht bzw. verbessert werden.

Ein weiterer Aspekt zur Verbesserung der Compliance Kultur ist die ethische Dimension des Compliance Managements. Durch die Erweiterung von Compliance Management von einem rein auf die Einhaltung rechtlicher Vorschriften ausgerichteten hin zu einem wertebasierten Compliance Management, welches die Ziele und Erwartungen der Stakeholder in die Konzeption von Compliance integriert, lässt sich auch die Akzeptanz und das Bewusstsein bei den eigenen Mitarbeitern steigern.¹⁵

Compliance ist heute in den meisten Unternehmen eine fest verankerte Disziplin, die aber in der Vergangenheit und insbesondere in der Zukunft einem großen Wandel unterliegt. Unternehmen müssen sich ständig an das regulatorische Umfeld anpassen und für sich erkennen, welche rechtlichen Themenfelder für das Unternehmen entscheidend sind um diese durch geeignete Managementsysteme zu steuern und weiter in Compliance zu investieren. Dies gilt natürlich insbesondere für die Unternehmen, die bisher nicht oder nur wenig in Compliance investiert haben, denn es gilt noch mehr als früher der Ausspruch des ehemaligen US-Staatsanwalts *Paul McNulty*: „*If you think compliance is expansive, try non-compliance*“.

In wirtschaftlich schwierigeren Zeiten müssen die Investitionen jedoch sinnvoll gewählt sein. Compliance Management muss dabei digitaler werden als dies bisher in den meisten Unternehmen der Fall ist; gleichzeitig müssen die einzelnen Systeme besser integriert werden, um den Anforderungen nach Effizienz aber auch Effektivität gerecht zu werden. Dazu müssen die Unternehmen konsequent ihre Prozesse auf solche Potentiale prüfen und hierbei sind Unterneh-

¹⁴ Vgl. ebenda.

¹⁵ Vgl. *Brendel/Herold/Schlegel*, CGO Magazin, Ausgabe 01/2020, S. 12–17.