LL.M.-Studium für Europäisches
und Internationales Wirtschaftsrecht

Master Thesis

zur Erlangung des akademischen Grades

LL.M. – Master of Laws

Compliance in der Industrie im Kontext der Europäischen Union

von

Olf-Jürgen Clemens Grofe, Dipl.-Jur. (Universität Münster)

eingereicht im Jänner 2015 an der
Rechtswissenschaftlichen Fakultät der Universität Wien
bei

ao. Univ.-Prof. Dr. Alina-Maria LENGAUER, LL.M.

Inhaltsverzeichnis

Abkürzungsverzeichnis 6
I. Einleitung 9
A. Ziel der Arbeit 13
B. Begriffsbestimmung 14
1. Eingrenzung 15
2. Corporate Compliance 16
a) Entwicklung 16
b) Definition 17
c) Corporate Governance und Corporate Compliance 17
3. Zwischenergebnis 18
II. Compliance im Unternehmen 19
A. Ziele von Compliance 19
1. Compliance Risiken 19
a) Beispiel Siemens 20
b) Strafrecht / Verwaltungsstrafrecht (Ordnungswidrigkeitenrecht) 21
aa) USA 22
bb) Europäische Union 23
cc) Großbritannien 24
dd) Deutschland 24
ee) Österreich 25
c) Kartellrecht 26
d) Öffentliches Vergaberecht 26
e) Weitere Folgen 28
2. ESMA - Leitlinien 29

3. Solvabilität II 31
4. Compliance matters 31
5. Literatur 32
B. Legislative Entwicklung zu Corporate Compliance in der EU 33
1. Internes Kontrollsystem 34
2. SOA 404 35
3. Abschlussprüfer-Richtlinie (EuroSOX) 35
4. Änderungsrichtlinie 37
5. Bisherige Erkenntnisse 38
6. Recht der einheitlichen europäischen Gesellschaftsformen 39
a) SE 40
b) SCE 41
c) EWIV 42
7. Pflicht der Leitung zur Einführung eines CMS 42
d) Begriff 42
e) Verpflichtung 43
aa) Meinungsstand 43
bb) Richtlinienkonforme Auslegung der nationalen Rechtslage 45
C. Compliance Management Systeme 49
1. CMS Standards 50
a) ISO 19600 – Compliance management systems – Guidelines 50
aa) ISO 50
bb) Allgemein zur ISO 19600 51
cc) Adressaten der ISO 19600 52
dd) Grundelemente eines CMS nach ISO 19600 53

(1) Schaffung der Voraussetzungen eines CMS nach ISO 19600 („Establish“ - Einrichten) 54
(2) Kontinuierlicher Verbesserungsprozess („Improve“ - Verbessern) 56
(a) Zentrale Elemente 56
(b) Develop – Implement – Evaluate – Maintain (PDCA Zyklus) 58
b) TR CMS 101:2011 59
aa) TÜV Rheinland 59
bb) Allgemein zum Standard TR CMS 101:2011 60
cc) Adressat des Standards TR CMS 101:2011 60
dd) Grundelemente eine CMS nach TR CMS 101:2011 62
c) ONR 192050:2013 02 01 64
aa) Austrian Standards Institute 65
bb) Allgemein zur ONR 192050 65
cc) Adressat 65
dd) Grundelemente eines CMS nach ONR 192050 66
d) IDW PS 980 67
aa) Institut der Wirtschaftsprüfer 67
bb) Allgemein zum Prüfungsstandard 68
cc) Adressat des Prüfungsstandards 69
dd) Grundelemente eine CMS nach IDW PS 980 70
2. Prüfung und Zertifizierung 72
a) Interne Audits 74
b) Externe Audits und Zertifizierungen 75
(1) Zertifizierung gem. ISO/IEC 17021 75
(2) Zertifizierung von ISO 19600 76
(3) Testat nach IDW PS 980 78

(4) Resümee 79
3. Zusammenfassender Vergleich 80
III. Ergebnisse und Ausblick 84
Literaturverzeichnis 90
Dokumente / Normen / Standards 96

ABKÜRZUNGSVERZEICHNIS

a.A.	andere Ansicht
AG	Die Aktiengesellschaft (Zeitschrift)
BB	Betriebs-Berater (Zeitschrift)
AEUV	Vertrag über die Arbeitsweise der europäischen Union
BDCO	Bundesverband Deutscher Compliance
BCM	Berufsverband der Compliance Manager
BVerfGE	Entscheidungssammlung des deutschen Bundesverfassungsgerichts
bzw.	beziehungsweise
CEO	Chief Executive Officer
CEN	Comité Européen de Normalisation (Europäisches Komitee für Normung)
CCO	Chief Compliance Officer
CCZ	Corporate Compliance Zeitschrift
CFO	Chief Financial Officer
CIS	Commonwealth of Independent States (Gemeinschaft Unabhängiger Staaten)
CMS	Compliance Management System
dAktG	Aktiengesetz (Deutschland)
DCGC	Deutscher Corporate Governance Codex
dGmbHG	Gesetz über die Gesellschaft mit beschränkter Haftung (Deutschland)
DoJ	Department of Justice
EIB	Europäische Investitionsbank
EWIV-VO	VERORDNUNG (EWG) Nr. 2137/85 DES RATES vom 25. Juli 1985 über die Schaffung einer Europaischen wirtschaftlichen Interessenvereinigung (EWIV)
ESMA	European Security and Markets Authority
FCPA	Foreign Corrupt Practices Act
f.	folgende (Singular)
ff.	folgende (Plural)

FTE	Full-Time-Equivalent
GmbHR	GmbH-Rundschau (Zeitschrift)
GWB	Gesetz gegen Wettbewerbsbeschränkungen (Deutschland)
ggf.	gegebenenfalls
HGB	Handelsgesetzbuch (Deutschland)
IDW	Institut der Wirtschaftsprüfer
IDW PS	Prüfungsstandard des Instituts der Wirtschaftsprüfer
IEC	International Electrotechnical Commission (Normungsgremium für Elektrotechnik)
IKS	Internes Kontrollsystem
iSd	Im Sinne des
ISO	International Organization for Standardization (Internationale Organisation für Normung)
ISO PC	ISO Project Committee
iVm	in Verbindung mit
KPI	Key Performance Indicator (Leistungskennzahl)
KMU	Kleine und mittlere Unternehmen
KWG	Kreditwesengesetz (Deutschland)
LG	Landgericht
MIFID	Market in Financial Instruments Directive (Richtlinie 2004/39/EG des Europäischen Parlaments und des Rates vom 21. April 2004 über Märkte für Finanzinstrumente)
Mio.	Millionen
NGO	Nichtregierungsorganisation
m.w.N.	mit weiteren Nachweisen
NYSE	New York Stock Exchange
NZG	Neue Zeitschrift für Gesellschaftsrecht (Zeitschrift)
öAktG	Aktiengesetz (Österreich)
ÖCGK	Österreichischer Corporate Governance Kodex
ÖCOV	Österreichische Compliance Officer Verbund
ÖGmbHG	Gesetz über die Gesellschaft mit beschränkter Haftung (Österreich)

OGAW	Organismus für gemeinsame Anlagen in Wertpapieren
ONR	ON-Regel
OWiG	Gesetz über Ordnungswidrigkeiten (Deutschland)
PDCA	Plan – Do – Check – Act (Planen – Durchführen – Überprüfen – Verbessern)
Rs.	Rechtssache
S.	Seite
SEC	Stock Exchange Commission
SE	Societas Europaea
SEAG	Ausführungsgesetz zur Societas Europaea (Deutschland)
SCE-VO	VERORDNUNG (EG) NR. 1435/2003 DES RATES vom 22. Juli 2003 über das Statut der Europäischen Genossenschaft (SCE)
SE-VO	VERORDNUNG (EG) Nr. 2157/2001 DES RATES vom 8. Oktober 2001 über das Statut der Europäischen Gesellschaft (SE)
s.o.	siehe oben
SOA	Sarbanes-Oxley-Act
TI	Transparancy International
TI CPI	Transparancy International Corruption Perception Index
VbVG	Österreichisches Bundesgesetz über die Verantwortlichkeit von Verbänden für Straftaten (Verbandsverantwortlichkeitsgesetz)
QM-System	Qualitätsmanagementsystem
UK	United Kingdom
VDB	Verband der Bahnindustrie in Deutschland
wbl	Wirtschaftsrechtliche Blätter (Zeitschrift)
z.B.	zum Beispiel
Zif.	Ziffer
ZIP	Zeitschrift für Wirtschaftsrecht (Zeitschrift)
ZIS	Zeitschrift für internationale Strafrechtsdogmatik
zit.	zitiert
ZRFC	Zeitschrift für Risk, Fraud & Compliance (Zeitschrift)

I. EINLEITUNG

„Die Siemens AG plant, ihre American Depositary Receipts von der New Yorker Börse zu delisten. Des Weiteren wird Siemens die Beendigung ihrer Berichtspflichten gegenüber der amerikanischen Securities and Exchange Commission vorbereiten (Deregistrierung). Diesen Beschluss fasste der Vorstand in seiner Sitzung am 27. Januar 2014."[1]

Diese Information hat die in der Siemens Aktiengesellschaft und ihren Konzerngesellschaften mit dem Thema Compliance beschäftigten Mitarbeiter[2] aufhorchen lassen. Immerhin war die Notierung an der NYSE nicht nur ein rechtliches Argument für die strafrechtliche Verfolgung der Siemens AG und dreier ihrer Tochtergesellschaften, sondern auch für Strafzahlungen in Höhe von mehreren hundert Millionen US-Dollar alleine in den USA sowie die Einführung eines weltweiten Compliance Systems im Konzern, das von Compliance Abteilungen überwacht wird.[3] Grund für diese Strafzahlungen in den Vereinigten Staaten von Amerika aber auch für Bußgelder in Deutschland waren Ermittlungen der US Börsenaufsicht, des US Justizministeriums und der Staatsanwaltschaft München, wegen langjähriger und systematischer Verstöße gegen Anti-Korruptionsgesetze und Buchführungsregeln in unterschiedlichen Geschäftsbereichen und mehreren Landesgesellschaften des Siemens-Konzerns.[4]

Entsprechend hat die Presseerklärung auch sofort klargestellt, dass weiterhin höchste Transparenz in der Finanzberichterstattung und erstklassige Corporate Governance bei Siemens oberste Priorität hätten. Das Ziel des Delistings und der Deregistrierung sei es, dem veränderten Verhalten der Investoren

[1] Presseerklärung der Siemens AG, München, 28.01.2014.
[2] Die weibliche Form ist der männlichen Form in dieser Arbeit gleichgestellt; lediglich aus Gründen der Vereinfachung wurde die männliche Form gewählt.
[3] Seit dem 12.März 2001 notierte die Siemens AG an der NYSE. Deswegen fiel Siemens gemäß dem Foreign Corrupt Practices Act von 1977 (15 U.S.C. §§ 78dd-1, ff.) als „issuer" unter die US-amerikanische Jurisdiktion. Die Einstellung der Verfahren in den USA erfolgte am 15.12.2008 gegen Zahlung von 450.000.000 US$.
[4] Moosmayer, S. 118.

Rechnung zu tragen. Als Konsequenz würden Prozesse der Finanzberichterstattung vereinfacht und deren Effizienz gesteigert.

Der „Bestechungsskandal“ bei Siemens war ein Grund, warum in den letzten Jahren der Begriff „Compliance“ auch in Europa alltäglich und zu einem Dauerbrenner in der Berichterstattung von verschiedensten Medien geworden ist. Beispiele, die das Thema Compliance international erstmals auf die Titelseiten brachten, sind die Bilanzskandale von Unternehmen wie Enron oder Worldcom in den Jahren 2001 und 2002.[5]

Namen vieler weiterer deutscher aber auch österreichischer Unternehmen sind in den letzten Jahren im Zusammenhang mit Compliance in der Presse erschienen. Im Wesentlichen ging es hier um Korruptionsfälle im Zusammenhang mit dem Abschluss von Verträgen,[6] um kartellrechtliche Themen (als Beispiele im Bereich der produzierenden Industrie seien nur die sogenannten „Schienenfreunde“ genannt, ein Kartell von Produzenten von Eisenbahnschienen[7] oder auch das „Schaltanlagenkartell“, bei dem gegen Siemens eine Geldbuße in Höhe von 396,56 Mio. Euro verhängt wurde[8]), aber auch um andere Verstöße zum Beispiel im Bereich des Datenschutzes[9] oder des Steuerrechts[10].

[5] Strauch, NZG 2003, 952: Diese waren die Ursache für die Verschärfung der US-Amerikanischen Federal Sentencing Guidelines[5] durch den Sarbanes Oxley Act.
[6] ein Beispiel aus der jüngeren Vergangenheit ist der Vorwurf gegenüber der deutschen Rüstungsfirma Krauss-Maffei Wegmann, die entsprechend eines Berichtes der Süddeutschen Zeitung vom 28.12.2013 für den Zuschlag eines Vertrages aus dem Jahr 2003 für die Lieferung von 170 Leopard 2 Panzern nach Griechenland einen Betrag von 1,7 Mil. EUR gezahlt haben soll, siehe unter: http://www.sueddeutsche.de/politik/ermittlungen-in-athen-griechischer-ex-politiker-gesteht-schmiergeld-deal-um-deutsche-panzer-1.1852195 (2.1.2014).
[7] siehe beispielsweise: http://de.wikipedia.org/wiki/Schienenfreunde (3.1.2014)
[8] EuGH, Urteil v. 19.12.2013, Gasisolierte Schaltanlagen-Kartell, Rs. C-239/11 P, C-489/11 P, C-498/11.
[9] siehe zB „Datenaffäre bei der Bahn: Konzern ließ heimlich 173.000 Mitarbeiter überprüfen“ (Süddeutsche Zeitung, 29.1.2009).
[10] siehe als Beispiel: „Banken tricksten Fiskus aus“ in http://www.zeit.de/wirtschaft/2013-11/banken-steuern-aktiengeschaefte (4.1.2014).

Die Beispiele zeigen, dass eine fehlende Compliance Kultur zu höchsten wirtschaftlichen Schäden bis hin zur Existenzgefährdung eines Unternehmens führen kann.

Als Folge der Aufdeckung und im Zuge der Aufarbeitung von Compliance Skandalen wurden und werden Compliance Einheiten in den Unternehmen geschaffen, die die Aufgabe haben, „Compliance“ in den Geschäftsprozessen zu implementieren.

Weitere Zeichen einer zunehmenden Bedeutung von Compliance im Wirtschaftsleben sind die Einrichtung von Lehrgängen und Seminaren sowie Studien zum Thema Compliance [11] aber auch die Schaffung eines eigenständigen Berufsbildes des sogenannten „Compliance-Officers“ bzw. des „Compliance Managers“.[12]

Wirtschaftsverbände unterstützen ihre Mitglieder bei der Einführung von Compliance in ihren Unternehmen, indem sie verschiedenste Leistungen rund um Compliance anbieten. So wurde im Verband der Bahnindustrie Deutschlands ein komplettes Compliance Paket geschnürt, dass aus einem VDB-Code of Conduct inklusive Begriffsklärungen und Umsetzungshilfe sowie Workshops, verbandsinterne Compliance-Leitlinie, Zusammenarbeit mit anderen Verbänden und der Deutschen Bahn AG sowie einem Handlungsleitfaden zum Thema kartellrechtskonforme Verbandsarbeit besteht.[13]

---

[11] siehe beispielsweise: Studiengang Compliance an der Deutschen Universität für Weiterbildung, http://www.duw-berlin.de/de/studiengaenge/compliance.html (3.1.2014); an der TU Ingolstadt das Studium Compliance and Corporate Governance, http://www.thi.de/studium/studienangebote/compliance-and-corporate-governance.html (3.1.2014); Studium zum Certified Compliance Expert an der School of Governance, Risk & Compliance – Steinbeis Hochschule Berlin (http://www.school-grc.de/studium/certified-compliance-expert.html).

[12] siehe die Beschreibung des Berufsbildes des Compliance Officers beispielsweise im Posistionspapier des Bundesverbands Deutscher Compliance Officer unter http://www.bdco.de/Publikationen/BDCO_PosP.pdf (3.1.2014) und die eines Compliance Managers unter http://berufenet.arbeitsagentur.de/berufe/start?dest=profession&prof-id=89949 (3.1.2014).

[13] Hagel/Dahlendorf, CCZ 2014, 275 (276ff.).

Inzwischen gibt es unterschiedliche Normen und Standards zu Compliance, welche die Basis für den Aufbau eines Compliance Systems aber auch für entsprechende Audits darstellen.[14] Auf internationaler Ebene gibt es bei der Internationalen Organisation für Normung (ISO) seit 2012 das Komitee „ISO PC 271 Compliance Management Systems“ dessen Sekretariat bei Standards Australia angesiedelt ist. Der vom Komitee beschlossene Schlussentwurf (Draft International Standard) zur ISO 19600[15] wurde am 11. Juli 2014 in Wien verabschiedet. Der finale Standard ISO 19600:2014(E) erschien in der weltweit gültigen Fassung im Dezember 2014.[16]

Die Anzahl der Publikationen zu Compliance nimmt mehr und mehr zu. Neben verschiedensten Aufsätzen zu Compliance-Themen in der betriebswirtschaftlichen und rechtswissenschaftlichen Literatur gibt es für den deutschen Rechtsraum seit 2008 die „Corporate Compliance Zeitschrift“ des Verlags C.H. Beck, die Kurzbeiträge, Fachaufsätze und relevante Gerichtsentscheidungen zu Compliance-Themen enthält. Vom Finance Magazin gibt es eine zweimonatlich erscheinende Online-Publikation namens „Compliance“.[17] In Österreich ist seit 2010 im LexisNexis Verlag die Zeitschrift „Compliance Praxis“ als Fachmagazin für den Bereich „Governance, Risk & Compliance“ erhältlich. [18] Unter anderem ist „Compliance Praxis“ das Publikationsorgan des im November 2013 gegründeten Vereins „Österreichische Compliance Officer Verbund“ (ÖCOV), dessen Zweck es ist, die Interessen von natürlichen und juristischen Personen zu vertreten, die im Compliance Bereich tätig sind.[19]

---

[14] z.B. Standards Australia „AS 3806 – Compliance Programs“; Standard für Compliance Management Systems des TÜV Rheinland (TR CMS 101:2011); Austrian Standards, ON-Regel "Compliance Managementsysteme - Anforderungen und Anleitung zur Anwendung" (ONR 192050); Institut der Wirtschaftsprüfer in Deutschland, Prüfungsstandard „Grundsätze der ordnungsgemäßen Prüfung von Compliance Management Systemen (IDW PS 980).
[15] ISO/DIS 19600:2014 (E) Compliance management systems – Guidelines.
[16] https://www.iso.org/obp/ui/#iso:std:iso:19600:ed-1:v1:en (13.12.2014) - im Folgenden ISO 19600 genannt.
[17] siehe unter http://compliance-plattform.de.
[18] http://www.compliance-praxis.at/Magazin/Mediadaten (3.1.2014).
[19] § 2 der Statuten des Vereins „Österreichische Compliance Officer Verbund“ (ÖCOV).

Andere hier zu nennende Verbände sind der im November 2012 aus dem „Frankfurter Compliance Kreis“ hervorgegangene „Bundesverband Deutscher Compliance Officer“ (BDCO), dessen Ziel es ist, Informationen zu Compliance-Themen zwischen Unternehmen, Mitgliedern, relevanten Behörden, Politik und anderen Verbänden zu transportieren.[20] Weiters gibt es den „Berufsverband der Compliance Manager“ (BCM), der nach eigenen Angaben die führende berufsständische Vereinigung für Compliance Manager und Compliance Verantwortliche aus Unternehmen, Verbänden und anderen Organisationen ist. Sein Ziel ist die Definition und Wahrnehmung der Interessen der Verbandsmitglieder.[21] Auch ist hier das Netzwerk Compliance e. V. in dem sich Corporate-Compliance-Experten aus verschiedenen Unternehmen mit dem Ziel zusammengeschlossen haben, um den Erfahrungsaustausch zu fördern, über aktuelle Herausforderungen zu diskutieren und gezielt Wissen zu vermitteln.[22] Vergleichbare Ziele verfolgt das Deutsche Institut für Compliance – DICO.[23]

A. Ziel der Arbeit

Diese in den letzten Jahren ersichtlich gestiegene Bedeutung von Compliance ist Anlass für meine Untersuchung von Rechtsquellen der Europäischen Union nach Normen, die einerseits vorgeben, was unter Compliance verstanden wird und andererseits, wie Compliance umzusetzen ist.

Wesentliche Rechtsquellen hierbei sind das primäre Gemeinschaftsrecht der Verträge aber auch Regelungen des sekundären Gemeinschaftsrechts, wie Verordnungen, Richtlinien und Beschlüsse, sei es als Gesetzgebungsakte (Art. 289 AEUV) oder in Form der delegierten Durchführungsrechtsakte der Kommission im Sinne des Art. 290 AEUV, als unverbindliche Rechtsakte (Empfehlungen/Stellungnahmen) oder im Wege sonstiger Handlungformen, die den Organen der Union zur Verfügung stehen.[24] In diesem Kontext soll jedoch

[20] Compliance Praxis 4/2012, 43.
[21] http://www.bvdcm.de/wer-wir-sind (3.1.2014).
[22] http://www.netzwerk-compliance.de/netzwerk-compliance-ev.html (12.12.2014).
[23] https://dico-ev.de/index.php?id=11 (15.12.2014).
[24] Näher hierzu Borchardt, § 5 C, Rz. 509ff.

nicht das nationale Recht – sei es europäischer Mitgliedsstaaten (insbesondere Deutschland und Österreich) oder der USA – außer Acht gelassen werden.

Die Praxis zeigt, dass es unterschiedliche Ausprägungen von Compliance in Wirtschaftsunternehmen gibt. Insbesondere fällt auf, dass zwischen den Aufgaben eines Compliance Officers in stark regulierten Bereichen wie Finanz- und Versicherungsunternehmen und solchen in Industrieunternehmen unterschieden werden kann. Der Fokus dieser Arbeit liegt auf Industrieunternehmen.

Ziel dieser Arbeit ist es, einerseits zu untersuchen, inwiefern das europäische Recht und entsprechende nationale Normen des Gesellschaftsrechts in Deutschland und Österreich zur Einrichtung eines CMS verpflichten. Andererseits sollen bestehende CMS-Standards dargestellt und verglichen werden. Zuletzt wird auf Basis der Erkenntnisse eine Handlungsempfehlung an Industrieunternehmen gegeben, die Verbesserungspotentiale in Sachen Compliance sehen und nutzen wollen und ein Blick in die Zukunft gewagt.

B. Begriffsbestimmung

Es handelt sich bei dem auch in der deutschen Sprache benutzten Begriff „Compliance“ um einen Anglizismus, der je nach Nutzungszusammenhang verschieden interpretiert wird. Das Subjektiv „Compliance“ bedeutet in der Übersetzung unter anderem „Befolgung“, „Einhaltung“, „Erfüllung“ und „Ordnungsmäßigkeit“, aber auch „Einverständnis“, „Einwilligung“ und „Unterwürfigkeit“. Der Begriff „in compliance“ wird übersetzt mit „in Übereinstimmung“.[25]

[25] http://dict.leo.org/#/search=compliance&searchLoc=0&resultOrder=basic&multiwordShowSingle=on (2.1.2014).

Die Nutzung des Begriffs Compliance erfolgt damit immer in einem individuellen Kontext. Welche Themenbereiche von Compliance erfasst sind, ist nur aus der jeweiligen Perspektive des Betroffenen zu definieren.[26]

1. Eingrenzung

Sucht man im Online-Lexikon Wikipedia nach dem Begriff „Compliance" bietet sich unter anderem die Auswahl zwischen Compliance (Medizin), Cross Compliance, IT-Compliance und Tax-Compliance.[27] Weiters finden sich regelmäßig Begriffe wie Criminal Compliance[28] und Corporate Compliance.

All diesen Begriffen ist gemeinsam, dass es um die Einhaltung von bestehenden Vorgaben geht. Im medizinischen aber auch psychologischen Kontext wird die Kooperationsbereitschaft des Patienten[29] bzw. der Grad des „konsequenten Befolgens der ärztlichen Ratschläge"[30] als „Compliance" bezeichnet.

Der Begriff der „Cross-Compliance" entspringt dem Bereich der Gemeinsamen Agrarpolitik der Europäischen Union.[31] Eine Legaldefinition findet sich in Erwägungsgrund 3 der Verordnung (EG) Nr. 73/2009 des Rates[32], wonach die Regelung der „Einhaltung anderweitiger Verpflichtungen" („Cross-Compliance") integraler Bestandteil der gemeinschaftlichen Unterstützung landwirtschaftlicher Betriebsinhaber in Form von Direktzahlungen ist.

---

[26] Kreuzer, CFOaktuell 2009, 205.
[27] http://de.wikipedia.org/wiki/Compliance (2.1.2014); Anmerkung: Der Begriff „Compliance (Recht)" ist nicht zu finden!
[28] siehe nur Rotsch, ZIS 2010, 614 ff.
[29] Petsche/Larcher in Petsche/Mair, S. 3.
[30] Busch/Hjertonsson, Sieben Elemente eines effizienten und wirksamen Compliance-Management-Systems, CFOaktuell 2013, 96 (96).
[31] VO (EG) 1782/2003, Art. 8 „Review" spricht in der englischen Fassung von „Cross Compliance", in der deutschen Fassung jedoch noch von der „Einhaltung anderweitiger Verpflichtungen".
[32] VERORDNUNG (EG) Nr. 73/2009 DES RATES vom 19. Januar 2009 mit gemeinsamen Regeln für Direktzahlungen im Rahmen der gemeinsamen Agrarpolitik und mit bestimmten Stützungsregelungen für Inhaber landwirtschaftlicher Betriebe und zur Änderung der Verordnungen (EG) Nr. 1290/2005, (EG) Nr. 247/2006, (EG) Nr. 378/2007 sowie zur Aufhebung der Verordnung (EG) Nr. 1782/2003.

Ebenso steht auch die IT-Compliance für die Einhaltung aller rechtlichen Rahmenbedingungen im Bereich der Informationstechnologie.[33] Dieser Ansatz gilt ebenfalls in der Tax-Compliance, jedoch konsequenterweise bezogen auf den Bereich des Steuerrechts.[34] Criminal Compliance wiederrum bezieht sich insbesondere auf die strafrechtlich pönalisierten Verpflichtungen von Wirtschaftsbeteiligten und die damit im Zusammenhang stehenden Fragen der Haftungsvermeidung.[35]

2. Corporate Compliance

Für die Industrie sind insbesondere die Compliance Begriffe relevant, die der Betriebswirtschaft und der wirtschaftsrechtlichen Terminologie zuzuordnen sind.

a) *Entwicklung*

In diesem Zusammenhang hat sich die sogenannte Corporate Compliance herausgebildet, die ihren Ursprung in der strafrechtlichen Verfolgung von Verstößen gegen das Wettbewerbsrecht durch US-amerikanische Unternehmen in den 1960er Jahren hat und auf deren Basis erste Corporate Compliance Codes eingeführt wurden.[36]

Besondere Bedeutung erlangte Compliance ab dem Ende der 1980er Jahre im Bereich des Bankwesens, wo es der Sicherstellung der Einhaltung der Vorgaben in den spezifischen Risikobereichen einer Bank diente.[37]

---

[33] Petsche/Larcher in Petsche/Mair, S. 5.
[34] Kindl/Petsche, Compliance-Praxis 1/2013, 14 (14).
[35] Dazu ausführlich Rotsch, ZIS 10/2010, 614 ff.
[36] Feltl/Pucher, wbl 2010, 265 (266). Einen solchen Compliance Code stellen auch die Siemens Business Conduct Guidelines dar. Diese definieren Compliance wie folgt: „Compliance bei Siemens ist die Einhaltung aller Bestimmungen, die unser Verhalten – auch gegenüber externen Anspruchsgruppen – regeln. Dies können extern vorgegebene Gesetze und Regelungen sein und/oder intern definierte Richtlinien, Verfahren und Kontrollen." (Siemens Business Conduct Guidelines, Edition 2009-01, S. 31, siehe auch unter http://www.siemens.com/sustainability/pool/cr-framework/business_conduct_guidelines_d.pdf (4.1.2014)).
[37] Feltl/Pucher, wbl 2010, 265 (266); Napokoj, Rz. 1ff., laut Napokoj verweist auch die Definition des Basel Committees on Banking Supervision auf freiwillige Verhaltensvorschriften (soft law) und ist insofern mit der Definition im DCGC vergleichbar.

b) ***Definition***

In diesen Bereich des Bank- und Kapitalmarktrechts fällt eine Legaldefinition des Compliance Begriffs in einer europäischen Rechtsnorm. So wird in der MiFID-Durchführungsrichtlinie Compliance als „Einhaltung der rechtlichen Vorgaben" definiert.[38] Fast diese Übersetzung ist auch in der deutschen Fassung der EG-Geldwäsche-Richtlinie[39] zu finden. Wo die deutschsprachige Richtlinie im 37. Erwägungsgrund davon spricht, dass sie „*eine Reihe detaillierterer zusätzlicher Anforderungen, etwa im Hinblick auf Strategien und Verfahren zur Gewährleistung der Einhaltung der einschlägigen Vorschriften*" enthält, heißt es in der englischen Fassung: „*This Directive establishes […..], and certain additional, more detailed requirements, such as the existence of compliance management procedures and policies".*[40]

c) ***Corporate Governance und Corporate Compliance***

Der Deutsche Corporate Governance Codex definiert in Regel 4.1.3. Compliance als die in der Verantwortung des Vorstands liegende Einhaltung der gesetzl. Bestimmungen und unternehmensinternen Richtlinien.[41] Im Gegensatz zum DCGC erwähnt der Österreichische Corporate Governance Kodex auch in seiner letzten Fassung vom Juli 2012 den Begriff Compliance in den Regeln 20, 21 und 44 nur im Zusammenhang mit der Emittenten-Compliance-Verordnung, also eingeschränkt auf den bank- und kapitalmarktrechtlichen Bereich.[42]

---

[38] 3. Erwägungsgrund der RICHTLINIE 2006/73/EG DER KOMMISSION vom 10. August 2006 zur Durchführung der Richtlinie 2004/39/EG des Europäischen Parlaments und des Rates in Bezug auf die organisatorischen Anforderungen an Wertpapierfirmen und die Bedingungen für die Ausübung ihrer Tätigkeit sowie in Bezug auf die Definition bestimmter Begriffe für die Zwecke der genannten Richtlinie.

[39] RICHTLINIE 2005/60/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 26. Oktober 2005 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung.

[40] Ebenso in Art. 34 I EG-Geldwäsche-Richtlinie: der englische Begriff „Compliance Management" wird in der deutschen Fassung mit „Gewährleistung der Einhaltung der einschlägigen Vorschriften" übersetzt.

[41] Diese Regelung ist auch im Recht der Societas Europaea anwendbar (Messow, S. 241).

[42] Feltl/Pucher, wbl 2010, 265 (267) – In der sogenannten L-Regel 15 (ÖCGK 2010) wird jedoch gefordert, dass der Vorstand "geeignete Vorkehrungen zur Sicherstellung der Einhaltung der für

Corporate Governance bezeichnet aus Sicht der Europäischen Kommission das Verhältnis zwischen der Führung eines Unternehmens, seinem Verwaltungsrat, Aktionären und anderen Interessengruppen. Sie bestimmt die Art und Weise, wie Unternehmen geführt und kontrolliert werden.[43] Corporate Governance Kodices sind Soft Law und geben neben zwingenden auch empfehlende Regeln wieder.[44] Unabhängig davon, ob nun nur rechtliche oder auch unternehmensinterne Vorgaben Compliance determinieren, ist Compliance Teil einer Corporate Governance, die als Querschnittsmaterie[45] alle Regelungen und Standards sorgfältiger Unternehmensführung beinhaltet.[46] Corporate Governance wird damit weiter verstanden, als Compliance. Dies gilt unabhängig davon, ob Compliance nun nur extern vorgegebene Gesetze und Regelungen oder auch intern definierte Richtlinien, Verfahren und Kontrollen umfasst.

Da sich Compliance nun aber im Alltag des Wirtschaftslebens eben auf alle Vorgaben bezieht, die für ein Unternehmen, sei es in der Industrie oder einem anderen Wirtschaftszweig, relevant sind, gibt es die unterschiedlichsten relevanten Normen, die je nach Wirtschaftszweig und Standort des Unternehmens zu identifizieren und anzuwenden sind.

3. Zwischenergebnis

Es gibt nicht den europäischen Compliance Begriff. In der Wirtschaftspraxis und der produzierenden Industrie bezieht sich Compliance jedenfalls auf die Einhaltung aller jeweiligen einzuhaltenden rechtlichen Vorgaben sowie der unternehmensinternen Richtlinien. Europarechtliche Legaldefinitionen gibt es

---

das Unternehmen relevanten Gesetze" zu treffen hat. Hieraus lässt sich nach Feltl/Pucher ableiten, dass dem Compliance-Gedanken auch im ÖCGK Rechnung getragen wird (m.w.N.). Zum gleichen Ergebnis kommen Petsche/Larcher in Petsche/Mair, S. 27f. jedoch unter Verweis auf Regeln 37 und 40 des ÖCGK.

[43] Aktionsplan Europäisches Gesellschaftsrecht und Corporate Governance – ein moderner Rechtsrahmen für engagiertere Aktionäre und besser überlebensfähige Unternehmen, Mitteilung COM(2012) 740 final, vom 12.12.2012, S. 3. mit Verweis auf OECD-Grundsätze auf dem Gebiet der Corporate Governance, 2004.

[44] Sturm, Kap. 3, III, 2, S. 60.

[45] Hausmaninger/Kletter/Burger, Einleitung, Rz. 4.

[46] Napokoj, Rz. 8.

lediglich im Bereich der gemeinsamen Agrarpolitik und im bank- und kapitalmarktrechtlichen Bereich. In beiden Fällen stimmen die Definitionen jedoch in Ihrem Mindestgehalt mit dem Verständnis des Deutschen Corporate Governance Codex überein. Compliance betrifft damit nicht nur die „typischen" Bestechungs- oder Kartellfälle, sondern geht viel weiter.

II. COMPLIANCE IM UNTERNEHMEN

A. Ziele von Compliance

Compliance Ziele können aus verschiedenen Perspektiven dargestellt bzw. verstanden werden. Im Folgenden soll nach einer Betrachtung der Sicht der Industrie auf die Sicht des europäischen Gesetzgebers und der Literatur eingegangen werden.

1. Compliance Risiken

Aus Sicht der Industrie gibt es unterschiedliche Motivationen, sich im Einklang mit Compliance zu verhalten und dies mittels eines CMS auch abzusichern. An erster Stelle hierbei steht wohl die Vermeidung von Compliance Risiken, die im Realisierungsfall erheblichen Einfluss auf das Geschäftsergebnis und die Zukunft des Unternehmens haben können.

Die Sicherstellung von Compliance kann aber darüber hinaus nicht nur Vertrauen von Stakeholdern (Aktionäre, Kunden, Gesellschaft) schaffen, sondern auch Arbeitnehmer durch klare und unmissverständliche Vorgaben motivieren. Auch sichert Compliance die Reputation des Unternehmens und kann dadurch einen Beitrag zur Werterhaltung leisten.[47]

Grundsätzlich sollte es aber eine Selbstverständlichkeit sein, dass Unternehmen, deren Eigentümer bzw. Geschäftsleiter sowie die Führungskräfte und Mitarbeiter eines Unternehmens im Einklang mit rechtlichen Vorgaben

[47] ONR 192050, Vorwort, S. 3.

sowie der unternehmensinternen Richtlinien handeln. Das Risiko, gegen diese Regulative zu verstoßen, ist als Compliance Risiko zu bezeichnen.[48] Die Vermeidung von Compliance Risiken ist aber nicht nur ethischer Selbstzweck, sondern verhindert auch erhebliche Kosten.

a) ***Beispiel Siemens***

Der Siemens Compliance Fall[49] soll als Beispiel für die erheblichen wirtschaftlichen Folgen dienen, die Compliance Verstöße nach sich ziehen können. Der Abschluss der gerichtlichen Verfahren in Deutschland und den USA[50] war nach Angaben von Siemens nur so schnell möglich, weil Siemens innerhalb von weniger als zwei Jahren neben der ermittlungstechnischen Aufarbeitung der Vergangenheit und der vollumfänglichen Kooperation mit den Behörden ein Compliance-Programm entwickelt und weltweit im gesamten Konzern implementiert hat.[51] Dies alles geschah aber nicht kostenlos.

Der Aufbau einer weltweiten Compliance Organisation binnen kürzester Zeit, der Umbau des Unternehmens, die Einführung eines konzernumfassenden internen Regelwerks und Kontrollen zu Compliance sowie interne Untersuchungen auch durch Rechtsanwaltskanzleien und Wirtschaftsprüfer verursachte Kosten in Milliardenhöhe. Daneben wurden Strafzahlungen in Höhe von 450 Mio. US$ und 596 Mio. EUR fällig. In einem von der SEC eingeleiteten Zivilverfahren stimmte Siemens einer Gewinnabschöpfung in Höhe von 350 Mio. US$ zu.

---

[48] Petsche-Toifl-Neiger-Jirges, S. 27: „Compliance-Risiko ist das Risiko eines Compliance-Verstoßes."
[49] s.o. S. 9.
[50] Am 15. Dezember 2008 gab die Siemens AG bekannt, dass die Verfahren wegen des Vorwurfs der Bestechung von Amtsträgern zeitgleich in München und Washington D.C. beendet wurden. Siehe Presseinformation unter http://www.siemens.com/press/pool/de/pressemitteilungen/corporate_communication/axx20081219d.pdf (30.10.2014) und die Information des DOJ vom 15.12.2008 unter http://www.justice.gov/archive/opa/pr/2008/December/08-crm-1105.html (05.11.2014).
[51] Moosmayer, S. 118.

Darüber hinaus schlägt ein Vergleich mit der Welt Bank mit einer Summe von 100 Mio. US$ zu Buche, die über einen Zeitraum von 15 Jahren zur Unterstützung der Bestechungsbekämpfung zu zahlen sind, einem freiwilligen zweijährigen Verzicht auf die Teilnahme an Ausschreibungen der Weltbank durch die Siemens AG und sämtlicher Tochtergesellschaften und verbundenen Unternehmen sowie einer bis zu vier Jahre andauernden Zulassungsentziehung für die russische Tochtergesellschaft von Siemens.[52]

Aufgrund des Vorwurfs von in der Vergangenheit erfolgten Verletzungen von Richtlinien der EIB zur Betrugsbekämpfung im Zusammenhang mit von der EIB finanzierten Projekten hat Siemens in einem Vergleich der EIB zugesagt, über einen Zeitraum von fünf Jahren internationale und zwischenstaatliche Organisationen, Nichtregierungsorganisationen, Wirtschaftsverbände und/oder wissenschaftliche Institutionen mit insgesamt 13,5 Mio. Euro zu finanzieren, die Projekte oder andere Initiativen zur Unterstützung verantwortungsvollen Handelns und Korruptionsbekämpfung unterstützen.[53]

b) ***Strafrecht / Verwaltungsstrafrecht (Ordnungswidrigkeitenrecht)***

Abhängig von Art, Ort und Umfang des Compliance Verstoßes kann die Folge der jeweiligen Pflichtverletzung das Unternehmen und die betroffenen Beteiligten treffen. Die rechtlichen Folgen solcher Compliance-Verstöße sind entsprechend vielfältig und sind unter anderem davon abhängig, ob im jeweiligen Unternehmen ein effektives Compliance Management System implementiert wurde.

---

[52] http://web.worldbank.org/WBSITE/EXTERNAL/NEWS/0,,contentMDK:22234882~pagePK:34370~piPK:34424~theSitePK:4607,00.html (5.11.2014) – aufgrund dieser Vereinbarung war es Siemens in Welt Bank finanzierten Ausschreibungen nicht möglich, als Bieter aufzutreten. Dieses „blacklisting“ ist ein erheblicher Nachteil im weltweiten Geschäft. Es ist davon auszugehen, dass es erhebliche Umsatzeinbußen zur Folge hatte.

[53] http://www.siemens.com/about/sustainability/de/themenfelder/compliance/collective-action/eib-and-siemens-settlement-agreement.htm (05.11.2014).

aa) USA

So binden beispielsweise die US-amerikanischen Federal Sentencing Guidelines aus dem Jahr 1991 die US-Gerichte bei der Strafzumessung, berücksichtigen aber bei der Ahndung von Vergehen eines Unternehmens das Vorhandensein eines effektiven Corporate Compliance-Programms strafmildernd.[54] Typische Beispiele aus dem US-amerikanischen Rechtsumfeld für Compliance-Verstöße finden sich im FCPA von 1977 und im Sarbanes Oxley Act, der in Folge der Finanzskandale von Enron und Worldcom in den USA im Jahre 2002 der Sarbanes-Oxley-Act als Bundesgesetz vom Kongress verabschiedet wurde.

Im FCPA werden sowohl die Bestechung ausländischer Amtsträger unter Strafe gestellt, als auch die nicht korrekte Buchführung beispielsweise durch die falsche Berücksichtigung von gezahlten Bestechungsgeldern als Provisionen, Lizenzgebühren, Beratungsgebühren, Vertriebskosten, etc.[55] Das Unternehmen kann im Falle der strafrechtlichen Verurteilung wegen Bestechung ausländischer Amtsträger je Fall eine Strafe von bis zu 2 Mio. US$ treffen und im Falle des Verstoßes gegen die Buchführungsvorschriften bis zu 25 Mio. US$.[56]

Ziel des Sarbanes-Oxley-Acts ist es, die Aktionäre und die Öffentlichkeit vor Fehlern im Rechnungswesen und betrügerischen Verhaltensweisen in Unternehmen zu schützen. Adressaten sind US-amerikanische und ausländische Unternehmen, deren Wertpapiere an US-Börsen (National Securities Exchanges) gehandelt werden, deren Wertpapiere mit Eigenkapitalcharakter (Equity Securities) in den USA außerbörslich gehandelt werden, oder deren Wertpapiere in den USA öffentlich angeboten werden (Public Offering). Weiters gilt es für deren Tochterunternehmen.

[54] Petsche in Petsche/Mair, S. 23; Moosmayer, S. 8 mit weiteren Nachweisen und Darstellung der Anforderungen an die Strafmilderung.
[55] FCPA – Resource Guide, S. 39 unter http://www.justice.gov/criminal/fraud/fcpa/guide.pdf (07.09.2014).
[56] ebenda, S. 68.

Gem. Sec. 304 SOA sind CEO und CFO eines Unternehmens bei falschem Abschlussbericht verpflichtet, erhaltene Boni und Abfindungen an das Unternehmen zurückzuzahlen. Unter den Voraussetzungen der Sec. 906 SOA bestehen strafrechtliche Sanktionen, die bei Absicht Geldstrafen bis zu 5 Mio. US-Dollar und Freiheitsstrafen bis zu 20 Jahren vorsehen![57]

bb) Europäische Union

Gemäß Artikel 83 AEUV kann die EU Richtlinien mit Mindestvorschriften zum EU-Strafrecht für die EU-Straftatbestände gem. Art. 83 I, S. 2 AEUV erlassen. Die geltenden Rechtsvorschriften der EU haben die Wahl der Art der Haftung juristischer Personen für begangene strafrechtliche Handlungen bisher immer den Mitgliedstaaten überlassen, da das Konzept der strafrechtlichen Haftung juristischer Personen nicht in allen nationalen Rechtsordnungen existiert.[58]

Das zweite Protokoll aufgrund von Artikel K.3 des Vertrags über die Europäische Union zum Übereinkommen über den Schutz der finanziellen Interessen der Europäischen Gemeinschaften[59] verpflichtet in Artikel 3 die Mitgliedstaaten zu den erforderlichen Maßnahmen, um sicherzustellen, das juristische Personen für Delikte des Betrugs, der Bestechung und der Geldwäsche zu Gunsten der juristischen Person von ihren Mitarbeitern verantwortlich gemacht werden können. Zum einen knüpft es die Haftung an die Begehung des Delikts durch eine Person in einer Führungsfunktion, zum anderen an die Begehung des Delikts durch eine Person in Mitarbeiterfunktion, wenn die Tat durch mangelnde Überwachung oder Kontrolle verursacht worden ist. Gem. Art. 4 des zweiten Protokolls sind gegen die juristischen Personen iSd Art. 3 wirksame, angemessene und abschreckende Sanktionen zu verhängen.

---

[57] Starke, S. 105ff.

[58] MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN RAT, DEN EUROPÄISCHEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS UND DEN AUSSCHUSS DER REGIONEN vom 20.9.2011, KOM(2011) 573 endgültig, S. 10.

[59] siehe unter http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:31997F0719(02)&from=DE (16.11.2014).

Eine Vielzahl europäischer Länder haben Gesetze über die strafrechtliche Verantwortung juristischer Personen eingeführt.[60] In allen Mitgliedsstaaten ist dies jedoch bisher nicht erfolgt. Auch nach Ansicht der Kommission bestanden daher – jedenfalls im Jahre 2011 – noch immer Lücken im geltenden Straf- und Verfahrensrecht, die einem wirksamen Vorgehen der Strafverfolgungsbehörden zum Schutz der finanziellen Interessen der Union im Wege stehen.[61]

cc) Großbritannien

Der in Großbritannien im Jahr 2011 in Kraft getretene UK Bribery Act stellt alle korruptiven Handlungen aller natürlichen und juristischen Personen, die geschäftlich in Großbritannien tätig sind unter Strafe und begründet eine strikte Haftung des Unternehmens für seine Repräsentanten (Mitarbeiter oder beauftragte Dritte). Auch hier gilt: die einzige Verteidigung des Unternehmens gegen einen Vorwurf des Verstoßes gegen den UK Bribery Act ist das Bestehen adäquater Prozesse, um Verstöße von Mitarbeitern oder Repräsentanten zu verhindern.[62]

dd) Deutschland

In Deutschland existiert (noch)[63] kein Unternehmensstrafrecht im engeren Sinne. Die Ahndung von Wirtschaftskriminalität, die nicht einzelnen bestimmten Personen zugeordnet werden kann, findet mit Hilfe des

[60] Aufzählung bei Römermann, GmbHR 2014, 1ff. (4).
[61] MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN RAT, DEN EUROPÄISCHEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS UND DEN AUSSCHUSS DER REGIONEN vom 26.5.2011, KOM (2011) 293 endgültig, S. 9 – siehe unter http://ec.europa.eu/justice/criminal/files/comm_pdf_com_2011_0293_f_communication_de.pdf (16.11.2014).
[62] Moosmayer, S. 10; UK Bribery Act Guidance, S. 15, siehe unter http://www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf (08.11.2014).
[63] Römermann, GmbHR 2014, 1ff. (4): am 18.09.2013 wurde vom Justizminister des deutschen Bundeslandes Nordrhein-Westfalen der Entwurf des Gesetzes zur Einführung der strafrechtlichen Verantwortlichkeit von Unternehmen und sonstigen Verbänden – Verbandsstrafgesetzbuch (VerbStrG) vorgestellt. Siehe hierzu unter http://www.justiz.nrw.de/JM/justizpolitik/jumiko/beschluesse/2013/herbstkonferenz13/zw3/TOP_II_5_Gesetzentwurf.pdf (16.11.2014).

Ordnungswidrigkeitenrechts statt.[64] Im Zusammenhang mit Haftungsrisiken sei beispielsweise auf § 30, 130, 9 OWiG hingewiesen, wonach einer juristischen Person oder Personenvereinigung Geldbußen von bis zu 10 Mio. EUR auferlegt werden können, wenn im Betrieb oder Unternehmen eine Zuwiderhandlung gegen Pflichten begangen wird, die den Inhaber treffen und deren Verletzung mit Strafe oder Geldbuße bedroht ist, der Inhaber vorsätzlich oder fahrlässig die ihm obliegende Aufsichtspflicht verletzt hat und die Zuwiderhandlung bei gehöriger Aufsicht verhindert oder wesentlich erschwert worden wäre. Gem. § 30 I OWiG[65] haftet das Unternehmen für die Straftat oder Ordnungswidrigkeit der dort genannten Organe, wenn dadurch die Pflichten, welche das Unternehmen treffen, verletzt worden sind oder das Unternehmen bereichert worden ist. Reicht das Höchstmaß von 10 Mio. Euro dafür nicht aus, kann es gem. § 30 III in Verbindung mit § 17 IV OWiG überschritten und eine höhere Geldbuße festgesetzt werden. Im Rahmen der Erhöhung des Bußgeldrahmens des § 30 OWiG wurde seitens des deutschen Bundesgesetzgebers in der Begründung festgestellt, dass die Gerichte bei der Bemessung der Geldbuße Compliance Anstrengungen der Unternehmen berücksichtigen können. Entgegen anderslautenden Forderungen wurde jedoch auf eine diesbezügliche Regelung im Gesetzestext selbst verzichtet.[66]

ee) Österreich

Österreich hat seit 2006 ein Verbandsverantwortlichkeitsgesetz. Dem Verband kann eine gem. § 4 VbVG in Tagessätzen zu bestimmende Geldbuße (maximal 180 Tagessätze bis zu 10.000 EUR) auferlegt werden, wenn er für eine Straftat gem. § 3 VbVG verantwortlich ist. Dies ist dann der Fall wenn Entscheidungsträger oder auch, in den in § 3 III VbVG definierten Fällen,

---

[64] Antwort der deutschen Bundesregierung auf die Kleine Anfrage der Abgeordneten Katja Keul, Nicole Maisch, Luise Amtsberg, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN – Drucksache 18/2056.

[65] Absätze in Gesetzen und sonstigen Normen werden durch römische Zahlen dargestellt.

[66] siehe hierzu Gesetzgebungsvorschlag für eine Änderung der §§ 30, 130 des Ordnungswidrigkeitengesetzes (OWiG) der Fachgruppe Compliance im Bundesverband der Unternehmensjuristen (BUJ) unter http://www.buj.net/resources/Server/Dateien/BUJ_begr%C3%BC%C3%9Ft_Stellungnahme_der_Bundesregierung.pdf (12.09.2014).

Mitarbeiter Straftaten zugunsten des Verbands begangen haben, oder durch die Tat Pflichten verletzt worden sind, die den Verband treffen. Verantwortlich ist der Verband, wenn nach § 3 III Nr. 2 VbVG Entscheidungsträger die nach den Umständen gebotene und zumutbare Sorgfalt außer Acht gelassen haben. Dies ist insbesondere dann der Fall, wenn sie wesentliche technische, organisatorische oder personelle Maßnahmen zur Verhinderung solcher Taten unterlassen haben. Die Beachtung von Compliance durch Einrichtung eines CMS kann daher als „Schutzschirm“ vor Strafverfolgung des Unternehmens wirken.[67]

c) *Kartellrecht*

Kartellrechtliche Verstöße gegen die Art. 101 und 102 AEUV können gem. Artikel 23 Absatz 2 Buchstabe a) der Verordnung (EG) Nr. 1/2003 mit Geldbußen bis max. 10% des im vorausgegangenen Geschäftsjahr erzielten Gesamtumsatzes geahndet werden. Diese Strafen sind dementsprechend so hoch, dass auch ein großes Unternehmen hierdurch in eine wirtschaftliche Krise gelangen kann. Unangenehm für Unternehmen im Vorfeld der Bestrafung sind die kartellrechtlichen Ermittlungen, auch im Wege sogenannter Dawn Raids. Dies sind Nachprüfungen in den Räumlichkeiten des Unternehmens gem. Art. 20 II VO 1/2003 oder gem. Art. 21 I VO 1/2003 in anderen Räumlichkeiten auf anderen Grundstücken oder in anderen Transportmitteln- darunter auch die Wohnungen von Unternehmensleitern und Mitgliedern der Aufsichts- und Leitungsorgane sowie sonstigen Mitarbeitern der betroffenen Unternehmen und Unternehmensvereinigungen.

d) *Öffentliches Vergaberecht*

Auf europäischer Ebene sind insbesondere bei Korruptionsfällen der Ausschluss von öffentlichen Ausschreibungen möglich. Art. 45 der RICHTLINIE 2004/18/EG über die Koordinierung der Verfahren zur Vergabe öffentlicher Bauaufträge, Lieferaufträge und Dienstleistungsaufträge fordert Bewerber oder

[67] Petsche/Trafoier, Compliance Praxis 2013, S. 6ff. (Heft 1).

Bieter von der Teilnahme an einem Vergabeverfahren auszuschließen, wenn der öffentliche Auftraggeber Kenntnis davon hat, dass dieser Bewerber oder Bieter wegen Beteiligung an einer kriminellen Organisation, Bestechung, Betrug oder Geldwäsche rechtskräftig verurteilt wurde. Vergleichbare Vorschriften gibt es in anderen Ausschreibungsbedingungen [68] sowie international in den Ausschreibungsbedingungen der weltweit engagierten Entwicklungsbanken[69].

Besondere Bedeutung in diesem Zusammenhang hat auch das sog. „Cross-Debarment-Agreement" der African Development Bank, der Asian Development Bank, der European Bank for Reconstruction and Development, der Inter-American Development Bank und der World Bank. [70] In diesem Vertrag vereinbaren die Entwicklungsbanken die gegenseitige Anerkennung der von Vergabeverfahren ausgeschlossen Unternehmen. Der hierdurch mögliche „Dominoeffekt" [71] kann beispielsweise für ein im Infrastrukturbereich international tätiges Industrieunternehmen existenzielle Folgen haben.

Es gibt im öffentlichen Bereich schwarze Listen und Korruptionsregister, die – sofern ein Unternehmen wegen entsprechender Korruptionsfälle auf diesen auftaucht, erhebliche wirtschaftliche Folgen, wie z.B. auch längerfristige Vergabesperren haben können. [72] So führt beispielsweise die deutsche Bundeshauptstadt ein Korruptionsregister, das der Information der öffentlichen Auftraggeber in Berlin über bekannt gewordene Verurteilungen von Unternehmen und der verantwortlich für sie handelnden Personen dient.

---

[68] für Deutschland siehe zB § 8a Nr. 5 VOB/A, § 7 Nr. 5 VOL/A.

[69] so wurde im Jahr 2006 die Joint International Financial Institutions (IFI) Anti-Corruption TaskForce der African Development Bank, Asian Development Bank, European Bank for Reconstruction and Development, European Investment Bank, International Monetary Fund, Inter-American Development Bank und Welt Bank gegründet, die auf Basis des gemeinsam beschlossenen UNIFORM FRAMEWORK FOR PREVENTING AND COMBATING FRAUD AND CORRUPTION ein koordiniertes Vorgehen gegen Betrug und Korruption vereinbart hat, http://www.afdb.org/fileadmin/uploads/afdb/Documents/Generic-Documents/30716700-EN-UNIFORM-FRAMEWORK-FOR-COMBATTING-FRAUD-V6.PDF (2.11.2014).

[70] "Agreement on Mutual Enforcement of Debarment Decisions" vom 9 April 2010 - http://lnadbg4.adb.org/oai001p.nsf/0/F77A326B818A19C548257853000C2B10/$FILE/cross-debarment-agreement.pdf (02.11.2014).

[71] Moosmayer, S. 16.

[72] Moosmayer, S. 14.

Gem. § 97 IV GWB sind öffentliche Aufträge an fachkundige, leistungsfähige sowie gesetzestreue und zuverlässige Unternehmen zu vergeben.[73] Das Berliner Korruptionsregister soll öffentliche Auftraggeber bei dieser ihnen obliegenden Prüfung der Zuverlässigkeit von Bieterinnen und Bietern, Bewerberinnen und Bewerbern sowie potentiellen Auftragnehmerinnen und Auftragnehmern unterstützen.[74] Korruption soll so wirksamer bekämpft und ihr vorgebeugt werden.[75]

e) ***Weitere Folgen***

Möglich sind weiters im Steuer- und Finanzrecht Konsequenzen wie Straf- und Verspätungszuschläge. Zu berücksichtigen sind mögliche Image- und Reputationsverlust durch Berichterstattung in der Presse und nicht zuletzt erhebliche Kosten im Zusammenhang mit Rechtsberatung und internen Aufklärung.

Zivilrechtlich darf die Gefahr des Schadenersatzes nicht aus den Augen gelassen werden. Zuletzt besondere Bedeutung erlangte das Schadenersatzrisiko gegenüber den geschädigten Kunden kartellierender Unternehmen im Zusammenhang mit den bereits erwähnten „Schienenfreunden“.[76] Auch von besonderer Bedeutung, insbesondere für die produzierende Industrie, ist die Gefahr der Produkthaftung und daraus resultierender Schadenersatzansprüche, bei Verstößen gegen Product Compliance Regelungen.

---

[73] Moosmayer, ebenda mit weiteren Beispielen.
[74] § 1 des Gesetzes zur Einrichtung und Führung eines Registers über korruptionsauffällige Unternehmen in Berlin (Korruptionsregistergesetz - KRG) - http://www.berlin.de/imperia/md/content/senatsverwaltungen/justiz/korruptionsregistergesetz.pdf?start&ts=1159364198&file=korruptionsregistergesetz.pdf (2.11.2014).
[75] http://www.stadtentwicklung.berlin.de/service/korruptionsregister/ (2.11.2014).
[76] s.o. Fn. 7 - Anspruchsgrundlage in Deutschland beispielsweise § 33 III GWB.

Interessant, aber in der Anwendung bisher weder in Deutschland[77] noch in Österreich[78] relevant, sind die Regelung des § 62 dGmbHG und § 86 öGmbHG. Die deutsche Regelung erlaubt die Auflösung einer GmbH, „wenn eine Gesellschaft das Gemeinwohl dadurch gefährdet, dass die Gesellschafter gesetzwidrige Beschlüsse fassen oder gesetzwidrige Handlungen der Geschäftsführer wissentlich geschehen lassen." Die österreichische Norm erlaubt die Auflösung, „wenn die Geschäftsführer im Betrieb des gesellschaftlichen Unternehmens sich einer gerichtlich strafbaren Handlung schuldig machen und nach der Art der begangenen strafbaren Handlung im Zusammenhalt mit dem Charakter des gesellschaftlichen Unternehmens von dem weiteren Betrieb desselben Missbrauch zu besorgen wäre."

Daneben sind ebenfalls die betroffenen Unternehmer als natürliche Person aber auch Organmitglieder und Mitarbeiter gefährdet, rechtliche Konsequenzen zu erleiden. Hier ist neben der strafrechtlichen Komponente auch das jeweilige zivilrechtliche Schadenersatzrisiko gegenüber dem Unternehmen sowie das Abberufungs- und Kündigungsrisiko der jeweiligen Organmitglieder und Mitarbeiter zu beachten.

Compliance Risiken können demzufolge aus Industriesicht eine hohe Relevanz im Hinblick auf den wirtschaftlichen Geschäftserfolg aber auch für den Unternehmer selbst – sei es der Eigentümer eines KMU oder der Aktionär einer großen börsennotierten Aktiengesellschaft – und die Organe bzw. deren Mitglieder sowie die beteiligten Mitarbeiter haben.

2. ESMA - Leitlinien

Aussagen zu den Zielen und der Funktion von Compliance im Unternehmen finden sich nur in wenigen spezifischen Dokumenten von Einrichtungen die der Europäischen Union zuzuordnen sind.

[77] Römermann, GmbHR 2014, 1ff. (2) – laut Römermann hat die Norm nicht einmal den „Status eines „ausgewachsenen Mauerblümchens". Außer einem Fall aus 1937 (KG Berlin, JW 1937, 1270) sei bisher keine Entscheidung eines deutschen Gerichts bekannt geworden.
[78] Reitenbach, S. 64.

Unter dem Datum des 25 Juni 2012 hat die ESMA[79] Leitlinien zu einigen Aspekten der MiFID-Anforderungen an die Compliance-Funktion bekannt gemacht. Zum Anwendungsbereich wird mitgeteilt, dass diese Leitlinien für Wertpapierfirmen (im Sinne der Begriffsbestimmung in Artikel 4 Absatz 1 Ziffer 1 der MiFID-Richtlinie [80]) einschließlich Kreditinstituten, die Wertpapierdienstleistungen erbringen, OGAW-Verwaltungsgesellschaften und die zuständigen Behörden gelten.

Die Leitlinie stellt keine absolute Vorgabe für diese Unternehmen dar, sondern dient dem Zweck praktische Erläuterungen zur Anwendbarkeit bestimmter Aspekte der MiFID-Anforderungen an die Compliance-Funktion zu geben, um eine gemeinsame, einheitliche und durchgängige Anwendung von Artikel 13 der MiFID-Richtlinie, Artikel 6 der MiFID-Durchführungsrichtlinie[81] sowie einzelner damit zusammenhängender Bestimmungen sicherzustellen.

Entsprechend der allgemeinen Leitlinie 1 - Punkt 14ff. - ist Aufgabe der Compliance Funktion im Unternehmen die Bewertung des Compliance-Risikos durch regelmäßige Risikoanalyse, sowie die Überwachungs- (allgemeine Leitlinie 2 - Punkt 18ff.), Berichterstattungs- (allgemeine Leitlinie 3 - Punkt 27ff.) und Beratungsfunktion (allgemeine Leitlinie 4 - Punkt 33ff.).

[79] Dokument ESMA / 2012 / 388 der Europäischen Wertpapier- und Marktaufsichtsbehörde - ESMA ist eine unabhängige EU-Behörde, die zur Stabilität des Finanzsystems in der EU beitragen soll, indem sie die Integrität, die Transparenz, die Effizienz und die Funktionsweise der Wertpapiermärkte sicherstellt und den Anlegerschutz intensiviert, siehe auch http://www.fma.gv.at/de/internationales/europaeische-aufsichtsarchitektur/esma.html (4.3.2014).
[80] Richtlinie 2004/39/EG des Europäischen Parlaments und des Rates vom 21. April 2004 über Märkte für Finanzinstrumente, zur Änderung der Richtlinien 85/611/EWG und 93/6/EWG des Rates und der Richtlinie 2000/12/EG des Europäischen Parlaments und des Rates und zur Aufhebung der Richtlinie 93/22/EWG des Rates.
[81] Richtlinie 2006/73/EG der Kommission vom 10. August 2006 zur Durchführung der Richtlinie 2004/39/EG des Europäischen Parlaments und des Rates in Bezug auf die organisatorischen Anforderungen an Wertpapierfirmen und die Bedingungen für die Ausübung ihrer Tätigkeit sowie in Bezug auf die Definition bestimmter Begriffe für die Zwecke der genannten Richtlinie.

3. Solvabilität II

Artikel 46 der Solvabilität II (Solvency II) Richtlinie[82] definiert die Compliance Funktion lediglich für die in den Anwendungsbereich der Richtlinie fallende Versicherungsunternehmen. Nach Art. 46 I der Solvabilität II Richtlinie ist Compliance auf die Überwachung der Einhaltung der Anforderungen gerichtet. Gemäß Absatz 2 gehört die Beratung des Verwaltungs-, Management- oder Aufsichtsorgans in Bezug auf die Einhaltung der in Übereinstimmung mit dieser Richtlinie erlassenen Rechts- und Verwaltungsvorschriften dazu.

Weitere Funktion ist die Beurteilung der möglichen Auswirkung von Änderungen des Rechtsumfelds auf die Tätigkeit des betreffenden Unternehmens sowie die Identifizierung und Beurteilung des mit der Nicht-Einhaltung der rechtlichen Vorgaben verbundenen Risikos.

4. Compliance matters

Im Jahre 2012 hat die Europäische Kommission eine Broschüre mit dem Titel “Compliance matters” herausgegeben. Diese Broschüre bezieht sich auf die Einhaltung der Regeln des Wettbewerbs- und Kartellrechts. Soweit in dieser Broschüre ausgeführt wird, welchen Zweck die Einhaltung der Regeln des Wettbewerbs- und Kartellrechts hat, wird – neben dem ethischen Aspekt der Compliance mit dem geltenden Recht – im Wesentlichen auf die Risiken verwiesen, die ein Verstoß gegen dieses Recht mit sich führen könnte. Einerseits wird hier die Gefahr der Verhängung von Geldbußen gegen Unternehmen und Unternehmensvereinigungen [83] hingewiesen. Andererseits wird auf die Möglichkeit der Mitgliedsstaaten verwiesen, auch natürliche Personen zu sanktionieren, wenn diese an Kartell-/Wettbewerbsverstößen beteiligt sind. Weiters werden als besondere Risiken die Nichtigkeit von

[82] RICHTLINIE 2009/138/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 25. November 2009 betreffend die Aufnahme und Ausübung der Versicherungs- und der Rückversicherungstätigkeit.
[83] s.o. S. 26 - Artikel 23 Absatz 2 Buchstabe a) der Verordnung (EG) Nr. 1/2003.

illegalen Vereinbarungen und schlechte Presse und andere Folgeschäden genannt.[84]

5. Literatur

Auch wenn sowohl die kartell- und wettbewerbsrechtliche Broschüre „Compliance matters“ als auch die ESMA-Leitlinien und die Solvabilität II-Richtlinie keine allgemeingültigen Vorgaben für andere Rechtsgebiete oder Wirtschaftszweige, die nicht unter ihren Anwendungsbereich fallen, darstellen, so sind die genannten Ziele von Compliance zu verallgemeinern und stimmen im Wesentlichen mit den folgenden, in der Literatur genannten Funktionen von Compliance überein.[85]

Besondere Bedeutung hat danach die *Schutzfunktion von Compliance*. Soweit Compliance vor Haftungs- und Reputationsrisken zu Lasten des Unternehmens, aber auch zu Lasten der Organe und Mitarbeiter schützt, dient es ebenso wie die Funktion des Risiko Managements, des internen Kontrollsystem (IKS) und der internen Revision und auch der Rechtsabteilung der Sicherung des Unternehmensbestands durch frühzeitige Erkennung von Risiken, die den nachhaltigen Erfolg des Unternehmens beeinträchtigen können und ermöglicht die Steuerung und Abwendung dieser Risiken. [86]

Diesem Leitziel folgen insbesondere auch die Funktionen der *Monitoring- und Überwachungsfunktion* und der *Beratungs-, Schulungs- und Informationsfunktion*. Nur eine ständige und nach aussen erkennbare Überwachung verbunden mit dem Angebot sowie – abhängig vom individduellen Unternehmen – möglicherweise auch die Verpflichtung der Mitarbeiter und des Managements zu Beratung, Information und auch zu

[84] Compliance matters, Europäische Union, Luxemburg 2012, S. 9ff.
[85] Insofern bei den Bezeichnungen der Funktionen völlig übereinstimmend (in den Erläuterungen jedoch teilweise abweichend) Napokoj, Rz. 11ff. und Kretschmer in Petsche/Mair, S.60ff.
[86] Napokoj, Rz. 42ff.; Petsche/Larcher in Petsche/Mair, S.7f.

Schulungen sichern den Schutz vor Haftungs- und Reputationsrisken nachhaltig.

Compliance hat daneben insbesondere bezogen auf eine laufende Weiterentwicklung und Optimierung von Prozessabläufen eine *Qualitätssicherungs- und Innovationsfunktion*.

Nicht zu unterschätzen und insbesondere für Unternehmen, die an öffentlichen Vergabeverfahren teilnehmen, die öffentliche Hand oder Sektorengesellschaften bedienen oder von öffentlichen Entwicklungsbanken finanziert werden, ist die Bedeutung von Compliance als *Marketingfunktion*. Unternehmen können nachweisen, gesetzestreue und zuverlässige Unternehmen zu sein (§ 97 IV GWB),[87] wenn sie ein funktionierendes Compliance Management System implementiert haben. Hierdurch können diese Unternehmen Wettbewerbsvorteile am Markt generieren.

B. Legislative Entwicklung zu Corporate Compliance in der EU

Corporate Compliance hat, ebenso wie auch die Funktion des Risiko Managements, im Unternehmen das Ziel der Vermeidung von Risiken, die den Unternehmensbestand und die Unternehmensziele gefährden, auch wenn diese bei Compliance auf die externen und unternehmensinternen Normen beschränkt sind. Das Gleiche gilt für das Interne Kontrollsystem,[88] das mit systematisch gestalteten technischen und organisatorischen Maßnahmen und Kontrollen die Einhaltung von Richtlinien und die Abwehr von Schäden bezweckt.

[87] s.o. S. 28.

[88] Unter dem IKS sind sämtliche Methoden und Maßnahmen im Unternehmen zu verstehen, die dazu dienen, das Vermögen zu sichern, die Genauigkeit und Zuverlässigkeit der Abrechnungsdaten zu gewährleisten und die Einhaltung der vorgeschriebenen Geschäftspolitik zu unterstützen; siehe Herzer/Strobl/Taufner in Hausmaninger/Gratzl/Justich, V., Rz. 117, m.w.N.

Sowohl Risiko Management, IKS und Compliance haben somit bei der Identifikation, Überwachung, Steuerung und Abwehr von unternehmensgefährdenden Risiken vergleichbare, wenn nicht oft die gleichen Ziele. Diese Nähe von internem Kontrollsystem, Risikoüberwachungssystem und Compliance zeigt sich auch im DCGC. Auf die schon erwähnte Regel 4.1.3, [89] wonach der Vorstand für die Einhaltung der gesetzlichen Bestimmungen und der unternehmensinternen Richtlinien zu sorgen hat und auf deren Beachtung durch die Konzernunternehmen hinwirkt, folgt in Ziffer 4.1.4 die Regelung wonach der Vorstand für ein angemessenes Risikomanagement und Risikocontrolling im Unternehmen sorgt.

Aufgrund dieser Gemeinsamkeiten liegt nahe, dass die Systeme auch einen gemeinsamen legislativen Ursprung haben.

1. Internes Kontrollsystem

Das Inkrafttreten des sogenannten „Konzern Transparenz Gesetzes“ in Deutschland hat im Jahre 1998 Vorstände von Aktiengesellschaften dazu verpflichtet, geeignete Maßnahmen zu setzen, insbesondere ein Überwachungssystem einzurichten, um den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkennen zu können (siehe § 91 II dAktG).

Auch wenn es zunächst nur die Aktiengesellschaft betraf, so sind aufgrund der anerkannten Ausstrahlungswirkung der Regelung auch die Geschäftsführer von Gesellschaften mit beschränkter Haftung hierdurch in die Pflicht gerufen.[90]

Eine vergleichbare Regelung wurde in Österreich im Jahre 1997 mit dem Unternehmensreorganisationsgesetz eingeführt, wonach der Vorstand der Aktiengesellschaft (§ 82 AktG) bzw. die Geschäftsführung (§ 22 Abs. 1 öGmbHG) unter anderem dafür zu sorgen hat, dass ein internes Kontrollsystem

[89] s.o. S. 17.
[90] Sartor/Bourauel, S. 16; wesentliche Regelungen in diesem Zusammenhang sind §§ 91, 93 dAktG, §§ 289, 315, 317, 321, 322 HGB.

geführt wird, das den Anforderungen des Unternehmens entspricht. Die Wirksamkeit dieses IKS ist durch den Prüfausschuss des Aufsichtsrates zu überwachen (§ 92 Abs. 4a, Zif. 2 öAktG).

2. SOA 404

Section 404 des Sarbanes-Oxley-Act von 2002[91] enthält Regelungen wonach jeder Jahresbericht eine Beurteilung des Managements über die Wirksamkeit des internen Kontrollsystems betreffend der Finanzberichterstattung durch die Geschäftsleitung des Unternehmens (Sec. 302 SOA) sowie ein Urteil des Wirtschaftsprüfers über die Wirksamkeit des internen Kontrollsystems enthalten muss. Ausländischen Unternehmen, die an US-Börsen gelistet waren, wurde Aufschub für die Erfüllung der Section 404 des Sarbanes-Oxley Acts gewährt. Diese mussten die Verpflichtungen grundsätzlich erst für jene Geschäftsjahre erfüllen, die nach dem 15. Juli 2006 endeten.

Der Sarbanes-Oxley-Act hat umfangreiche Pflichten auch für nicht in den USA ansässige Unternehmen geschaffen.[92] Es mussten interne Kontrollprozesse geschaffen werden, die in jährlichen internen und externen Audits zu überprüfen sind. Der hiermit verbundene Aufwand ist immens.

3. Abschlussprüfer-Richtlinie (EuroSOX)

Die 8. EU- Richtlinie („Abschlussprüfer-Richtlinie"),[93] welche 2006 in Kraft trat und bis 29. Juni 2008 in nationales Recht umzusetzen war, nimmt Änderungen an bestehenden Richtlinien aus den Jahren 1978, 1983 und 1984 vor. Zusammengefasst werden diese Anpassungen auch als EuroSOX bezeichnet.

---

[91] s.o. S. 22.
[92] s.o. Fn. 3.
[93] RICHTLINIE 2006/43/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 17. Mai 2006 über Abschlussprüfungen von Jahresabschlüssen und konsolidierten Abschlüssen, zur Änderung der Richtlinien 78/660/EWG und 83/349/EWG des Rates und zur Aufhebung der Richtlinie 84/253/EWG des Rates.

Ein Ziel der Richtlinie ist die Stärkung des Vertrauens der Öffentlichkeit in die Buch- und Bilanzführung der europäischen Unternehmen und Vermeidung länderübergreifende Finanzskandale durch Harmonisierung der Anforderungen an die von Abschlussprüfern zu erbringende Qualitat und Fachkunde[94] sowie ihrer Unabhängigkeit.[95] Bedeutsam im Zusammenhang mit Compliance ist die Definition von strengeren Anforderungen für die Abschlussprüfung des Jahresabschlusses oder konsolidierten Abschlusses von Unternehmen im öffentlichen Interesse. [96] In diesem Zusammenhang wird im 24. Erwägungsgrund der Abschlussprüfer-Richtlinie als Zweck der Prüfungsausschüsse und wirksamer interner Kontrollsysteme die Begrenzung finanzieller und betrieblicher Risiken sowie des Risikos von Vorschriftenverstößen auf ein Mindestmaß genannt.

Art. 41 I der Abschlussprüfer-Richtlinie sieht vor, dass jedes der in Art. 2 Nr. 13 Abschlussprüfer-Richtlinie definierten „Unternehmen von öffentlichem Interesse“[97] einen Prüfungsausschuss zu bilden hat, der je nach Festlegung des Mitgliedsstaates aus nicht an der Geschäftsführung beteiligten unabhängigen Mitgliedern des Verwaltungsorgans und/oder des Aufsichtsorgans des geprüften Unternehmens und/oder Mitgliedern zusammensetzen sollen, die durch Mehrheitsentscheidung von der Gesellschafterversammlung des geprüften Unternehmens bestellt werden.

Die Aufgabe des Prüfungsausschusses besteht gem. Art. 41 II, lit b) der Abschlussprüfer-Richtlinie unter anderem darin, die Wirksamkeit des internen

[94] 5. Erwägungsgrund der Abschlussprüfer-Richtlinie.
[95] siehe z.B. 9. und 11. Erwägungsgrund der Abschlussprüfer-Richtlinie.
[96] 23. Erwägungsgrund der Abschlussprüfer-Richtlinie.
[97] Art. 2 Nr. 13 Abschlussprüfer-Richtlinie definiert „Unternehmen von öffentlichem Interesse“ als Unternehmen, die unter das Recht eines Mitgliedstaats fallen und deren übertragbare Wertpapiere zum Handel auf einem geregelten Markt eines Mitgliedstaats im Sinne von Artikel 4 Absatz 1 Nummer 14 der Richtlinie 2004/39/EG zugelassen sind (börsennotierte Unternehmen), Kreditinstitute im Sinne von Artikel 1 Nummer 1 der Richtlinie 2000/12/EG des Europäischen Parlaments und des Rates vom 20. März 2000 über die Aufnahme und Ausübung der Tätigkeit der Kreditinstitute und Versicherungsunternehmen im Sinne von Artikel 2 Absatz 1 der Richtlinie 91/674/EWG.

Kontrollsystems, gegebenenfalls des internen Revisionssystems, und des Risikomanagementsystems des Unternehmens zu überwachen.

Wie in Sec. 404 SOA wird in der Abschlussprüfer-Richtlinie damit das Vorhandensein eines internen Kontrollsystems gefordert bzw. vorausgesetzt. Wie sich aus dem 24. Erwägungsgrund ergibt, setzt die Kommission voraus, dass ein Ziel des internen Kontrollsystems die Begrenzung des Risikos von Vorschriftenverstößen auf ein Mindestmaß ist.

4. Änderungsrichtlinie

Der Abschlussprüfer-Richtlinie schloss sich keine 2 Monate später die Änderungsrichtlinie[98] an. Ein wesentliches Ziel der Änderungsrichtlinie ist die Begründung einer kollektiven Verantwortung der Mitglieder der Verwaltungs-, Leitungs- und Aufsichtsorgane gegenüber der Gesellschaft für die Aufstellung und Veröffentlichung des Jahresabschlusses und des Lageberichts. Gem. Art. 1, Nr. 7 der Änderungsrichtlinie wurde die Jahresabschluss Richtlinie[99] durch Einfügung eines neuen Art. 46a geändert. Inhalt des neuen Art. 46a ist unter anderem die Verpflichtung von Gesellschaften deren Wertpapiere an einem geregelten Markt gehandelt werden, um die Aufnahme einer Erklärung im Lagebericht zum Corporate Governance Kodex, dem die jeweilige Gesellschaft unterliegt (Art. 46a I, lit. a) der Jahresabschluss Richtlinie) sowie auch eine die Beschreibung der wichtigsten Merkmale des internen Kontroll- und des Risikomanagementsystems der Gesellschaft im Hinblick auf den Rechnungslegungsprozess (Art. 46a I, lit. c) der Jahresabschluss Richtlinie).

[98] RICHTLINIE 2006/46/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 14. Juni 2006 zur Änderung der Richtlinien des Rates 78/660/EWG über den Jahresabschluss von Gesellschaften bestimmter Rechtsformen, 83/349/EWG über den konsolidierten Abschluss, 86/635/EWG über den Jahresabschluss und den konsolidierten Abschluss von Banken und anderen Finanzinstituten und 91/674/EWG über den Jahresabschluss und den konsolidierten Abschluss von Versicherungsunternehmen.

[99] VIERTE RICHTLINIE DES RATES vom 25. Juli 1978 aufgrund von Artikel 54 Absatz 3 Buchstabe g) des Vertrages über den Jahresabschluss von Gesellschaften bestimmter Rechtsformen (78/660/EWG).

Einerseits bestärkte diese Änderung jedenfalls für am Wertpapiermarkt notierte Unternehmen die Bedeutung der internen Kontroll- und Risikomanagementsysteme und knüpft somit an die Abschlussprüfer Richtlinie an und andererseits wird die Bedeutung von Corporate Governance durch eine Aufnahme der entsprechenden Erklärungen in den Lagebericht betont.

Art. 1, Nr. 8 der Änderungsrichtlinie sieht vor, dass in der Jahresabschluss-Richtlinie ein neuer Abschnitt 10a eingefügt wird, der die Pflicht und Haftung der Mitglieder der Verwaltungs-, Leitungs- und Aufsichtsorgane hinsichtlich der Aufstellung und der Veröffentlichung der Jahresabschlüsse und des Lageberichts betrifft. Entsprechend des neuen Art. 50b der Jahresabschluss-Richtlinie haben die Mitgliedstaaten sicherzustellen, dass die Mitglieder der vorgenannten Organe kollektiv zur Erstellung und Veröffentlichung von korrekten Jahresabschlüssen, Lageberichten und der Erklärungen zur Unternehmensführung verpflichtet sind. Art. 50c der Jahresabschluss-Richtlinie verpflichtet die Mitgliedsstaaten die Haftung der Organe ggü. den Gesellschaften sicherzustellen.

Auch hier wird – wie im SOA – das Ziel der Regelung deutlich, die Verantwortung der Organe der betroffenen Gesellschaften hervorzuheben, auch wenn dies nicht mit Mitteln des Strafrechts wie in SOA geschieht.

5. Bisherige Erkenntnisse

Wie bereits ausgeführt, wird im 24. Erwägungsgrund der Abschlussprüfer-Richtlinie als Zweck der Prüfungsausschüsse und wirksamer interner Kontrollsysteme die Begrenzung finanzieller und betrieblicher Risiken sowie des Risikos von Vorschriftenverstößen auf ein Mindestmaß genannt. Das IKS soll demzufolge zur Reduktion des Risikos von Vorschriftenverstößen (im Ergebnis also von Compliance-Risiken) führen.

Auch die Europäische Kommission hat im Kommissionsvorschlag zur Abschlussprüfer-Richtlinie[100] zum IKS ausgeführt, dass „ein derartiges System geeignete Konzepte und Verfahren voraussetzt, die eine prompte Weiterleitung verlässlicher Informationen und die Einhaltung der geltenden Rechts- und Verwaltungsvorschriften gewährleisten und die ordnungsgemäße Verwendung des Unternehmensvermögens sicherstellen. Der Prüfungsausschuss hat darüber zu wachen, dass Kontrollen durchgeführt werden und bei Verstößen gegen interne Kontrollregelungen oder Rechts- und Verwaltungsvorschriften geeignete Meldeverfahren greifen.“ Auch die Kommission hat damit Systeme zur Kontrolle der Einhaltung von Rechts- und Verwaltungsvorschriften als Teil des IKS gesehen.[101]

Die Bedeutung der internen Kontroll- und Risikomanagementsysteme wurde nochmals betont, indem die Änderungsrichtlinie Gesellschaften deren Wertpapiere an einem geregelten Markt gehandelt werden verpflichtet hat, dieses IKS im Lagebericht zu erläutern.

6. Recht der einheitlichen europäischen Gesellschaftsformen

Allgemein gültige Regelungen zur Klärung der Frage, ob und welche Pflichten im Hinblick auf die Einführung und Umsetzung von Compliance Management Systemen im Unternehmen bestehen, sind im einheitlichen europäischen Gesellschaftsrecht nicht zu finden.

[100] Vorschlag für eine Richtlinie des europäischen Parlaments und des Rates über die Prüfung des Jahresabschlusses und des konsolidierten Abschlusses und zur Änderung der Richtlinien 78/660/EWG und 83/349/EWG des Rates vom 16.3.2004, KOM(2004) 177 endgültig.

[101] Hier besteht Übereinstimmung mit den deutschen Regelungen für Wertpapierdienstleistungsunternehmen. Gemäß dem Rundschreiben über die Mindestanforderungen an die Compliance-Funktion und die weiteren Verhaltens-, Organisations- und Transparenzpflichten nach §§ 31 ff. WpHG für Wertpapierdienstleistungsunternehmen der deutschen Bundesanstalt für Finanzdienstleistungsaufsicht (MaComp), Modul AT 7 Ziff. 2, ist die „Compliance-Funktion ist Bestandteil des internen Kontrollsystems nach § 25a Abs. 1 Satz 3 Nr. 3 KWG“.

Im Wesentlichen können hier nur Verweise in das nationale Gesellschaftsrecht weiterhelfen, die sich jedoch auf die spezifische Pflichten des Vorstands bzw. des Verwaltungsrates und der Geschäftsführer beschränken.[102]

a) ***SE***

Im monistischen System der Societas Europaea führt gemäß Art. 43 I, S. 1 SE-VO der Verwaltungsrat die Geschäfte der SE. Da die Verordnung weder direkte noch indirekte Aussagen zu Compliance und Sorgfaltpflichten trifft, gilt der Verweis des Art. 9 SE-VO auf die nationalen Ausführungsgesetze. In Österreich gilt neben § 55 SEG die Regelung des § 39 SEG.

§ 55 SEG verweist auf § 84 öAktG, wonach die Vorstandsmitglieder der Gesellschaft gegenüber verpflichtet sind, die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden. Den vergleichbaren Verweis in das deutsche Recht der Aktiengesellschaft (§ 93 I dAktG) liefert § 39 SEAG.

Gemäß § 39 I SEG leitet der Verwaltungsrat die Gesellschaft und führt deren Geschäfte, wie es das Wohl des Unternehmens unter Berücksichtigung der Interessen der Aktionäre und der Arbeitnehmer sowie des öffentlichen Interesses erfordert. Weiters gilt § 39 III SEG wonach der Verwaltungsrat dafür zu sorgen hat, dass ein Rechnungswesen und ein IKS geführt werden, die den Anforderungen des Unternehmens entsprechen (siehe auch § 82 öAktG). Dieser Regelung entspricht in Deutschland § 22 III SEAG. Hiernach hat der Verwaltungsrat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden. Diese Regelung entspricht im Wesentlichen § 91 II dAktG.[103]

[102] Diese Verweise werden hier am Beispiel des deutschen und österreichischen Rechts dargestellt.
[103] Habersack/Drinhausen/Verse, § 22 SEAG, Rz. 28.

Im dualistischen System gilt Art. 39 I SE-VO: Hiernach führt das Leitungsorgan die Geschäfte der SE in eigener Verantwortung unter denselben Voraussetzungen, wie sie für Aktiengesellschaften mit Sitz im Hoheitsgebiet des betreffenden Mitgliedstaates gelten, führt bzw. führen. Auch diesbezüglich gelten die bereits erwähnten nationalen Regeln der §§ 82, 84 öAktG bzw. §§ 91 II, 93 I dAktG.

Damit werden – wie bei den nationalen Aktiengesellschaften Deutschlands und Österreichs – auch bei der SE mit Sitz in diesen Ländern die grundlegenden Verpflichtungen für ein internes Kontroll- bzw. Überwachungssystem geschaffen.

b) ***SCE***

Wie auch die SE sieht die SCE-VO gemäß der in der Satzung gewählten Form für die Europäische Genossenschaft in Art. 36, lit. b) SCE-VO entweder ein Leitungs- und ein Aufsichtsorgan (dualistisches System) oder ein Verwaltungsorgan (monistisches System) vor. Im dualistischen System führt das Leitungsorgan die Geschäfte in eigener Verantwortung (Art. 37 I, S. 1 SCE-VO), im monistischen System gilt das jeweilige Ausführungsgesetze über Art. 8 I, lit.c) i) SCE-VO.

Auch hier verweist § 21 SCE-AG (Deutschland) zur Sorgfaltspflicht und Verantwortlichkeit der Verwaltungsratsmitglieder auf § 34 des deutschen Genossenschaftsgesetzes, wonach die Vorstandsmitglieder bei ihrer Geschäftsführung die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters einer Genossenschaft anzuwenden haben.

In den österreichischen Regelungen hat eine aufsichtsratspflichtige Genossenschaft (§ 24 I Genossenschaftsgesetz) ein den Anforderungen des Unternehmens entsprechendes IKS einzurichten. § 24 I SCE-Gesetz sieht vor, dass diese Regelung auch für die monistische SCE gilt. Gem. § 24 II SCE-Gesetz kommen Rechte und Pflichten des Vorstands oder Aufsichtsrats einer

Genossenschaft im monistischen System dem Verwaltungsrat zu, sofern sie nicht geschäftsführenden Direktoren zugewiesen werden.

c) *EWIV*

Trotz der Qualifizierung der EWIV als Personen-(Handels-)gesellschaft gilt gem. Art. 20 I EWIV-VO der Grundsatz der Fremdvertretung durch einen Geschäftsführer. Die im Wortlaut gleichen Regelungen des § 5 I, S. 1 EWIV-Ausführungsgesetz (Deutschland) und § 6 I, S. 1 EWIV-Ausführungsgesetz (Österreich) verweisen sohin darauf, dass diese die Geschäftsführer die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden haben.[104]

7. Pflicht der Leitung zur Einführung eines CMS

d) *Begriff*

So wenig wie es eine unzweifelhafte und umfassende Legaldefinition von Compliance gibt, so wenig hilft uns der Gesetzgeber bei der Bedeutung des Begriffes des Compliance Management Systems. Der Begriff „Compliance Management" bezeichnet nach Petsche/Larcher die Gesamtheit aller zumutbaren Maßnahmen, die das regelkonforme Verhalten eines Unternehmens, seiner Leitungs- und Aufsichtsorgane, sowie seiner Organisationsmitglieder im Hinblick auf alle gesetzlichen Ge- und Verbote begründen.[105]

Die ONR 192015 definiert ein CMS als ein „Management-System zur Erreichung von Compliance".[106] Demzufolge stellt ein CMS die methodisch verknüpfte Aufgabe der Leitungsfunktionen im Unternehmen dar, um das Ziel

[104] Habersack, § 11, Rz. 21; im Wesentlichen stimmen diese Regelungen mit denen der GmbH-Gesetze überein, wonach die Geschäftsführer „in den Angelegenheiten der Gesellschaft" (so § 43 I GmbHG (Deutschland)) bzw. „der Gesellschaft gegenüber" (§ 25 I GmbHG (Österreich)) die Sorgfalt eines ordentlichen Geschäftsmannes anzuwenden haben."
[105] Petsche/Larcher in Petsche/Mair, S. 30.
[106] ONR 192050, S. 4.

„Erreichung von Compliance“ und die hiermit verbundenen Subziele zu definieren, zu setzen, zu steuern und zu kontrollieren.[107]

Der IDW PS 980 definiert das CMS als „sämtliche auf der Grundlage der definierten Unternehmensziele eingeführten Grundsätze und Maßnahmen eines Unternehmens, die auf die Sicherstellung eines regelkonformen Verhaltens der gesetzlichen Vertreter und der Mitarbeiter sowie ggf. von Dritten abzielen“.[108]

e) ***Verpflichtung***

Deutlich wurde bisher, dass sich diese Pflicht nicht unmittelbar aus dem untersuchten österreichischen oder deutschen Recht ergibt. Dennoch wird diese Frage gerade im Zusammenhang mit den Leitungsaufgaben des Vorstands der Aktiengesellschaft diskutiert.

aa) Meinungsstand

Teilweise wird vertreten, dass die Verpflichtung zur Einrichtung von Compliance Management Systemen unmittelbar aus der Leitungsaufgabe des Vorstands resultiere. Auch wenn eine klare Verpflichtung zur Einrichtung einer Compliance Organisation fehle, sei der hinter Einzelvorschriften des deutschen (§ 52a II BImSchG, § 130 OWiG, § 14 GeldwäscheG) aber auch des europäischen Rechts (Art. 11 EG-Geldwäsche-Richtlinie) stehende Rechtsgedanke zu verallgemeinern. Die Verpflichtung zum Aufbau einer Compliance Organisation sei aus einer Rechtsanalogie zu den vorgenannten Normen herzuleiten.[109]

Andere wollen die Grundlage für die Einrichtung der Compliancefunktion in § 91 II dAktG iVm § 317 IV dAktG erkennen. Die Prüfung des

---

[107] Managementsysteme beschreiben die Aufgaben des Managements, also der Leitungsfunktionen im Unternehmen, und verknüpfen Methoden, um die Management-Aufgaben Ziele setzen, steuern und kontrollieren erfolgreich zu bewältigen; http://de.wikipedia.org/wiki/Managementsystem (15.4.2014).

[108] IDW PS 980, S. 2-3; Die Übersetzung des Begriffs „Compliance Management“ in Art. 34 I EG-Geldwäsche-Richtlinie durch „Gewährleistung der Einhaltung der einschlägigen Vorschriften“ ist gemessen an diesen Erläuterungen wohl zu kurz.

[109] Schneider, ZIP 2003, 645 (649).

Risikofrüherkennungssystems sei Teil der Abschlussprüfung des Wirtschaftsprüfers und nur die Verortung der Pflicht zur Einrichtung einer Compliance Organisation in § 91 II dAktG sichere die Einbeziehung der Compliance in die Abschlussprüfung ab. Dies sei dann nicht der Fall, wenn diese Pflicht als Ausfluss aus der allgemeinen Geschäftsleitungsverantwortung der §§ 76 I, 93 I dAktG gesehen werde. [110]

Eine weitere Ansicht sieht die Grundlage für Compliance jedoch in genau diesen vorgenannten Regelungen des deutschen Aktienrechts. Der Wortlaut des § 91 II dAktG verlange lediglich ein Risikofrüherkennungssystem, nicht jedoch ein Management System im weiteren Sinne. Compliance beinhalte nicht lediglich die Früherkennung bestandsgefährdender rechtlicher Risken, sondern darüber hinaus die Identifikation und Umsetzung entsprechender Maßnahmen zur Beseitigung dieser Risken.[111]

Demgegenüber wird auch vertreten, dass eine allgemeine gesetzliche Verpflichtung nicht bestehe. Aus dem Vorliegen der erwähnten Spezialvorschriften lasse sich nicht schließen, dass eine generelle Pflicht zur Einrichtung einer wie auch immer gearteten Compliance Organisation bestehe. [112] Die Einhaltung der gesetzlichen Bestimmungen durch das Unternehmen sei eine Selbstverständlichkeit. Wie der Vorstand dies sicherstelle, obliege seinem Ermessen. Ob eine Compliance Organisation einzurichten ist, ist danach abhängig vom Compliance Risiko. Dieses sei abhängig von Faktoren wie Größe, Struktur und Lage des Unternehmens, dem Risikopotential seiner Märkte und dem jeweiligen Kapitalmarktzugang. [113] Hinzu kommen Verdachtsfälle der Vergangenheit (Gefährdungslage, die sich in der Vergangeheit realisiert hat), Art und Volumen der angebotenen Leistungen

[110] Dreher, FS Hüffer, S. 162ff, (169).
[111] Kölner Kommentar – Mertens/Cahn, § 91, 34ff.
[112] Hauschka/Hauschka, Abschnitt 1., § 1, Rz. 22 ff.; Napokoj, Rz. 31ff.; Petsche/Mair/Larcher verweist auf S. 26 auf die Ausnahme nach § 18 Wertpapieraufsichtsgesetz.
[113] MüKo-Spindler, § 91, Rz. 36.

(Branche, Geschäftsfeld), Kundenstruktur und Organisations- und Entwicklungsstand der IT und Controlling Systeme.[114]

Auch in Österreich leitet der Vorstand gem. § 70 I öAktG die Gesellschaft in eigener Verantwortung. Die Vorstandsmitglieder einer Aktiengesellschaft haben die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden (§ 84 I 1 öAktG). Ein Unterschied zur deutschen Rechtslage ist zu erkennen, wenn in der österreichischen Regelung des § 82, 2. Alt. öAktG statt eines Systems zur Erkennung bestandsgefährdender Risiken die Einrichtung eines IKS gefordert wird. Nichtsdestotrotz sind die erläuterten Meinungen ebenso in der österreichischen Rechtsordnung vertretbar.

bb) Richtlinienkonforme Auslegung der nationalen Rechtslage

Die vorgenannten Regelungen betreffen alle den Umfang der Pflichten des Vorstands im Rahmen der Leitung des Unternehmens und zur Begrenzung finanzieller und betrieblicher Risiken sowie des Risikos von Vorschriftenverstößen. Dies ist auch das Ziel der Abschlussprüfer Richtlinie.[115]

Art. 4 III EUV verpflichtet die Mitgliedsstaaten der EU unter anderem, alle geeigneten Maßnahmen zur Erfüllung der Verpflichtungen, die sich aus den Verträgen oder den Handlungen der Organe der Union ergeben zu ergreifen.

Wie der EuGH bereits in der Rechtssache „*Costa/Enel*“ entschieden hat, haben die Mitgliedsstaaten Souveränitätsrechte auf die Gemeinschaft übertragen. Das gemeinsame Recht gelte einheitlich und vollständig und könne nicht mehr einseitig rückgängig gemacht werden.[116] Der hieraus resultierende Vorrang des Unionsrechts gegenüber dem nationalen Rechts gilt jedenfalls dort, wo sich die europäischen Organe in den Grenzen der ihnen eingeräumten Hoheitsrechte

[114] Markfort, ZRFC 2014, 180 (181) in der Besprechung von LG München I v. 10.12.2013 - 5HK O 1387/10, AG 2014, 332-336.
[115] s.o. S. 35ff.
[116] EuGH, Rs. 6/64, Costa/Enel, Slg. 1964, 1251 (1269/1270).

bewegen. [117] Aus diesem Grundsatz folgt iVm Art. 288 III AEUV die Verpflichtung zur richtlinienkonformen Auslegung des nationalen Rechts. Art. 288 III AEUV verpflichtet die Mitgliedsstaaten und deren Organe zur Umsetzung der Richtlinien. Hieraus wird hergeleitet, dass auch nationale Vorschriften richtlinienkonform auszulegen sind,[118] wobei unerheblich ist, ob das nationale Recht vor oder nach dem Inkrafttreten der jeweiligen Richtlinie erlassen wurde.[119]

Es hat sich gezeigt, dass nationale Ausführungsgesetze zu EWIV, SE und SCE so wie auch die vergleichbaren Regelungen des Gesellschaftsrechts in Deutschland und Österreich sowohl auf die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters referenzieren, als auch im Rahmen der Ausformung der Leitungsaufgaben entweder ein IKS oder ein zumindest ein Überwachungssystem vorsehen, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.

Bei den europäischen wie bei den nationalen Gesellschaftsformen in Österreich und Deutschland hat die Geschäftsleitung daher die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiter anzuwenden und/oder ein internes Kontrollsystem bzw. ein Überwachungssystem einzurichten, um den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkennen zu können.

Compliance ist – wie bereits festgestellt[120] - Teil einer ordentlichen Corporate Governance.[121] Es ist eines der erklärten Ziele der Europäischen Kommission den Rechtsrahmen für „Corporate Governance“ zu reformieren. Zwar haben weder die Europäische Kommission noch das Europäische Parlament in den

[117] BVerfGE 89, 155/195; Borchardt, § 4, Rz. 145 kritisiert diese einschränkende Auslegung, da hiermit jeder nationalen Stelle ein Freibrief erteilt werde, dem Unionsrecht entgegenstehendes nationale Recht anzuwenden und damit Vorrang des Unionsrechts abzulehnen.
[118] EuGH, Rs. 14/83, „Von Colson und Kamann“, Slg. 1984, 1891.
[119] EuGH, Rs. C-106/89, Marleasing, Slg. 1990, I-4135.
[120] s.o. S. 18.
[121] Schneider, ZIP 2003, 645 (647); MüKo-Spindler, § 91, Rz. 35, m.w.N.

diesbezüglichen Veröffentlichungen[122] das Thema Compliance erwähnt, [123] jedoch wird auch im europarechtlichen Kontext Compliance als Bestandteil der Unternehmenskontrolle zur Leitungsaufgabe der jeweiligen Unternehmensleitung zu zählen sein[124].

Wie die Überlegungen zum Zweck von Compliance gezeigt haben, dient Compliance unter anderem der Vermeidung von spezifischen Compliance Risiken für das Unternehmen. Verstöße von Organmitgliedern und Unternehmensangehörigen können zu bestandsgefährdenden Risiken gehören.[125]

„Unternehmen von öffentlichem Interesse" haben gemäß Art. 41 I der Abschlussprüfer-Richtlinie einen Prüfungsausschuss zu bilden. Da der Prüfungsausschuss nach Art. 41 II lit. b) Abschlussprüfer-Richtlinie die Prüfung des IKS zur Aufgabe hat, kann somit angenommen werden, dass die Richtlinie voraussetzt, dass jedenfalls

- Systeme, die Compliance im Unternehmen zum Ziel haben, Teil des IKS sind[126] und
- Unternehmen im öffentlichen Interesse iSd Art. 2 Nr. 13 Abschlussprüfer-Richtlinie (also Aktiengesellschaften und Societas Europaea, deren Aktien an Börsen gehandelt werden, Kreditunternehmen und

[122] GRÜNBUCH Europäischer Corporate Governance-Rahmen vom 5.4.2011 (final) unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0164:FIN:DE:PDF (16.4.2014) und Aktionsplan Europäisches Gesellschaftsrecht und Corporate Governance - ein moderner Rechtsrahmen für engagiertere Aktionäre und besser überlebensfähige Unternehmen (s.o. Fn. 43); Entschließung des Europäischen Parlaments vom 29. März 2012 zu einem Corporate Governance-Rahmen für europäische Unternehmen (2011/2181(INI)), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P7-TA-2012-0118+0+DOC+PDF+V0//DE (16.4.2014).

[123] In der Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses vom 22./23. Mai 2013 zum in der vorhergehenden Fußnote erwähnten Aktionsplan ist der Berichterstatter Edouard de Lamaze unter 2.1, 1. Spiegelstrich der Ansicht, dass der Aktionsplan eine Politik der Vielfalt in der Zusammensetzung der Verwaltungsräte und der Politik zur Steuerung nichtfinanzieller Risiken (strategische und operative Risiken sowie Compliance-Risiko) fordere. (http://edz.bib.uni-mannheim.de/edz/doku/wsa/2013/ces-2013-0982-de.pdf) (10.10.2014) - Diese Definition ist jedoch nicht im Aktionsplan enthalten.

[124] MüKo-Spindler, § 91, Rz. 35; Hüffer, § 76, Rz. 9a, jeweils mit einer Vielzahl weiterer Nachweise.

[125] MüKo-Spindler, § 91, Rz. 35; Donner, CFOaktuell 2012, 20 ff. m.w.N.

[126] s.o. S. 38f.

Versicherungsunternehmen) ein IKS und damit auch ein System, das Compliance im Unternehmen zum Ziel hat, einzuführen haben.

Unternehmen, die nicht zu den vorgenannten Unternehmen des öffentlichen Interesses gehören, werden nicht durch die Abschlussprüferrichtlinie erfasst. Sofern weder der europäische noch der nationale Gesetzgeber die Einrichtung eines CMS verpflichtend vorsieht, gelten jedoch die allgemeinen Regelungen zu den Verpflichtungen der jeweiligen Geschäftsleitung – sei es des Vorstands, des Verwaltungsrates oder der Geschäftsführung. Gemein ist allen diesen Verpflichtungen die Anwendung der Sorgfalt eine ordentlichen und gewissenhaften Geschäftsführers, der das Unternehmen zu schützen und Schaden abzuwenden hat.

In diesem Zusammenhang gilt die Pflicht der Geschäftsleitung zur Legalitätskontrolle, wonach dafür Sorge zu tragen ist, dass Gebote und Verbote zu beachten sind, um das Unternehmen vor Schäden zu bewahren. Danach trifft die Leitung eine unternehmensweite Organisationsverantwortung und die Verpflichtung, auf ein rechtmäßiges Verhalten aller Unternehmensangehörigen auf allen Ebenen des Unternehmens hinzuwirken.[127]

Aufgrund dieser Obliegenheit ist der jeweilige Geschäftsleiter verpflichtet, auch auf die jeweiligen Compliance Risiken des von ihm geleiteten Unternehmens zu reagieren.

Erfordert nach objektiver Beurteilung die Risikosituation die Einrichtung eines CMS, so besteht aufgrund der genannten Regelungen des nationalen Rechts auch die Verpflichtung, im jeweils erforderlichen und angemessenen Umfang ein solches einzuführen. Unabhängig von der jeweiligen Risikosituation bzw. bei

[127] siehe auch Feltl/Pucher, wbl 2010, 265 (26268f.) mit Bezug auf die Aktiengesellschaft in Österreich; zur deutschen Rechtslage Markfort, ZRFC 2014, 180 (181) in der Besprechung von LG München I v. 10.12.2013 - 5HK O 1387/10, AG 2014, 332-336.m.w.N.

Fehlen einer abstrakten Gefährdungslage eine allgemeine Pflicht zur Einrichtung eines CMS anzunehmen, ginge aber zu weit.[128]

C. Compliance Management Systeme

Das Compliance Risiko hängt im Hinblick auf Wahrscheinlichkeit und Auswirkung von einer Vielzahl von Faktoren ab. Insbesondere sind hier die Art des jeweiligen Geschäfts und der Grad der Komplexität der jeweils zu beachtenden Vorschriften, aber auch die Größe, Branche, Anzahl der Mitarbeiter und die Frequenz früherer Vorfälle zu nennen.[129] Weiters relevant sind Themen wie zum Beispiel Zuordnung der Kunden zum öffentlichen oder privaten Sektor,[130] Börsenzulassung in den USA[131] sowie die Art und Weise des Kundenzugangs (eigene Mitarbeiter oder Handelsvertreter) oder die jeweiligen Orte der Geschäftstätigkeit.[132]

Es muss nicht nur das Ziel eines jeden Geschäftsleiters sein, eine durchgängige Bewertung des individuellen Compliance-Risikos durch regelmäßige Analyse der bestehenden Compliance-Risiken vorzunehmen, sondern es ist – zum Wohle des Unternehmens, der Eigentümer und Mitarbeiter – seine Verpflichtung, für diese Compliance – sei es im Rahmen eines IKS, eines Früherkennungssystems, mittels eines standardisierten CMS oder auf sonstige Art und Weise – zu sorgen.

---

[128] so auch Markfort, ZRFC 2014, 180 (181) in der Besprechung von LG München I v. 10.12.2013 - 5HK O 1387/10, AG 2014, 332-336.

[129] Hauschka/Hauschka, Abschnitt 1., § 1, Rz. 23. Im Übrigen siehe auch Markfort, ZRFC 2014, 180 (181) in der Besprechung von LG München I v. 10.12.2013 - 5HK O 1387/10, AG 2014, 332-336.

[130] in den meisten Rechtsordnungen unterliegen Amtsträger strengeren Vorschriften im Hinblick auf unzulässige Zuwendungen (Bestechungen) als Mitarbeiter des privaten Sektors.

[131] 15 U.S.C. §§ 78dd-1, ff., s.o. Fn. 3.

[132] Wie sich aus dem weltweiten Korruptionswahrnehmungsindex (Corruption Perception Index) der NGO Transparency International ergibt, besteht eine unterschiedliche Wahrnehmung, wie korrupt Politik und Verwaltung im Vergleich zu anderen Ländern wahrgenommen werden. Aus dem jeweiligen Rang eines Landes im Vergleich zu den anderen Ländern wird das jeweilige Korruptionsrisiko ermittelt. Der TI CPI 2013 ist unter http://cpi.transparency.org/cpi2013/results (15.4.2014) zu finden.

1. CMS Standards

Im Folgenden werden der internationale Standard ISO 19600 und drei im deutschsprachigen Raum bekannte und angewandte CMS Standards vorgestellt.

Zu nennen sind hier der TR CMS 101:2011 vom TÜV Rheinland, die Austrian Standards, ON-Regel "Compliance Managementsysteme - Anforderungen und Anleitung zur Anwendung" (ONR 192050) sowie der IDW PS 980 vom deutschen Institut der Wirtschaftsprüfer.

Sodann erfolgt ein zusammenfassender Vergleich auf Basis der vorhergehenden Erkenntnisse.[133]

a) *ISO 19600 – Compliance management systems – Guidelines*

Am 11. Juli 2014 wurde in Wien der Entwurf der ISO 19600 („Compliance Management Systems“) vom zuständigen Project Committee 271 der ISO verabschiedet[134]. Eine Veröffentlichung dieses Standards erfolgte im Dezember 2014.[135]Ziel dieses Standards ist eine verstärkte internationale Harmonisierung von Compliance-Management-Systemen.

aa) ISO

Die International Organization for Standardization ist die 1946 gegründete internationale Vereinigung von Normungsorganisationen. Sie erarbeitet internationale Normen in unterschiedlichsten Bereichen.[136] ISO hat Mitglieder

[133] nicht betrachtet in diesem Zusammenhang werden der auf Korruptionsbekämpfung ausgerichtete UK Bribery Act 2010, und der U.S. Foreign Corrupt Practices Act – FCPA.
[134] noch unter der Bezeichnung „DRAFT INTERNATIONAL STANDARD“ – ISO DIS 19600).
[135] s.o. Fn. 15f.
[136] Mit Ausnahme der Elektrik, der Elektronik und der Telekommunikation. Für diese Gebiete sind die Internationale elektrotechnische Kommission (IEC) und die Internationale Fernmeldeunion (ITU) zuständig. Alle drei Organisationen sind in der WSC (World Standards Cooperation) zusammengeschlossen. Siehe auch unter http://de.wikipedia.org/wiki/Internationale_Organisation_f%C3%BCr_Normung (27.09.2014).

aus 165 Ländern und ist eine unabhängige NGO. Mitglieder sind die national für Normierung zuständigen Organisationen.[137] Jedes Mitglied repräsentiert ISO im Ursprungsland. Sitz von ISO ist Genf (Schweiz).[138]

bb) Allgemein zur ISO 19600

Bemerkenswert ist, dass ISO 19600 keine zwingenden Voraussetzungen im Sinne von sogenannten Anforderungen („Requirements“) enthält, sondern als Leitfaden („Guidelines“) konzipiert ist.[139] „Requirements“ sind verbindliche Anforderungen einer Norm, die verpflichtend einzuhalten sind, wenn eine Organisation sich entscheidet, dem jeweils normierten Management System zu folgen.[140] Die Anerkennung der ISO 19600 als „Requirement Standard“ scheiterte am Widerstand verschiedener Mitglieder des ISO PC 271.[141]

Ein Grund hierfür mag gewesen sein, dass die Anforderungen an Compliance und CMS auch durch nationale Rechtssysteme geprägt werden. Seitens der Gegner der Anerkennung der ISO 19600 als Requirement Standard wird vertreten, dass das Ziel insbesondere auch immer die Vermeidung einer persönlichen Haftung im Unternehmen und des Unternehmens selbst sei. Da dies immer eine Frage wäre, die nach nationalem Recht zu entscheiden sei, sei schon der Nutzen einer nationalen Norm fraglich. Erst recht gelte dies für eine internationale Compliance Norm.[142] Die Komplexität der Norm sei insbesondere

---

[137] http://www.iso.org/iso/home/about/iso_members.htm (27.09.2014).
[138] http://www.iso.org/iso/about/about (27.09.2014).
[139] Ehnert, Compliance Praxis (Deutschland), 58 f. (59).
[140] In einer englischsprachigen Norm wird dies durch das Wort „shall“ ausgedrückt. Diese Form der verbindlichen Anforderungen kommt in der Guideline ISO 19600 nicht vor. – siehe ISO/TMB Joint Technical Coordination Group – „JTCG Frequently Asked Questions in support of Annex SL“ – Doc. No. JTCG N359, FAQ 24, S. 8, unter http://isotc.iso.org/livelink/livelink/16764161/ISO-TMB-JTCG_N0359_N0359__JTCG_FAQ_to_support_Annex_SL.pdf?func=doc.Fetch&nodeid=16764161 (06.10.2014).
[141] Petsche/Dechant, Compliance Praxis 2014, 14 (Heft 3).
[142] Ehnert, Compliance Praxis (Deutschland), 58 f. (58).

für kleine und mittlere Unternehmen ein Grund der gegen die Entwicklung eines effektiven CMS in solchen Organisation spräche.[143]

Demgegenüber ist die globale Industrielandschaft und die damit verbundenen internationale Konzernstrukturen jedoch ein wesentlicher Grund, der für eine internationale Norm spricht. Durch eine internationale Norm wird das gemeinsame Verständnis in der Zusammenarbeit mit Partnern und Lieferanten aus anderen Regionen gestärkt.[144] Die Norm vermittelt einen Grundkonsens. Die Anpassung des Standards an die nationalen rechtlichen Erfordernisse kann und muss aber auf nationaler Ebene erfolgen.

cc) Adressaten der ISO 19600

Die ISO 19600 ist als internationaler Standard grenzüberschreitend anwendbar. Ebenso wie die anderen oben dargestellten CMS-Standards erhebt die ISO 19600 in Ziffer 1 den Anspruch der Universalität, also der Anwendbarkeit auf alle Organisationsformen.[145]

Der Standard hat mit ca. 50 Klauseln und 27 Seiten einen hohen Detaillierungsgrad und Umfang. Da es sich bei der ISO 19600 um einen Leitfaden handelt, wird die Norm als Rahmenwerk flexibler, international konsistenter Vorgaben verstanden, das sich in bereits bestehende Compliance Programme eingliedern lasse.[146]

An der Einhaltung der sogenannten „High Level Structure“[147] der ISO 19600 zeigt sich aber, dass die Vorschläge der Norm sich nicht nur in ein bestehendes

[143] Stellungnahme des deutschen „Bundesverband der Unternehmensjuristen e.V.“, siehe unter http://www.buj.net/resources/Server/BUJ-Stellungnahmen/Stellungnahme-ISO-Standard.pdf, (09.10.2014).
[144] so auch Makowicz, Compliance Praxis (Deutschland), 33ff. (34).
[145] Der Begriff “Organization” (Organisation) ist in Ziffer 3.01 der ISO 19600 wie folgt definiert „person or group of people that has its own functions with responsibilities, authorities and relationships to achieve ist objectives“.
[146] Petsche/Dechant, Compliance Praxis 2014, 14 (Heft 3).
[147] High Level Structure bedeutet in diesem Zusammenhang, dass die Gliederung der Vorlage für Management System Standards gem. ISO/IEC Directives, Part 1, Consolidated ISO

Compliance-Programm eingliedern lassen (Upgrade), sondern auch in bereits bestehende Management-Systeme, die einen anderen Fokus haben. Hat eine Organisation daher beispielsweise schon die „ISO/IEC 27001 – Information security management systems – Requirements“ implementiert, so ist es aufgrund der einheitlichen Normenstruktur und damit einheitlicher Grundanforderungen weniger aufwendig, auch andere an der High Level Structure ausgerichtete Management-Systeme, wie ein CMS, dass den Leitlinien der ISO 19600 folgt, einzuführen.

Nachdem ISO Standards in der globalen Industriegesellschaft eine hohe Anerkennung genießen und aus dem nationalen bzw. regionalen Kontext heraustreten, kann davon ausgegangen werden, dass zukünftig auch die internationale Anerkennung steigen wird.

Die ISO 19600 kann daher zukünftig besonders für internationale Industriekonzerne, Zulieferanten und Partner eine so hohe Bedeutung erlangen, dass diese damit auch vorrangige Anwender des Standards werden.

dd) Grundelemente eines CMS nach ISO 19600

ISO 19600 folgt ebenso wie andere Management Systeme dem Deming-Kreis oder auch PDCA-Zyklus (Plan – Do – Check – Act)[148] und fordert einen kontinuierlichen Verbesserungsprozess.

Supplement, 2014, Annex SL folgt; siehe unter http://isotc.iso.org/livelink/livelink/fetch/2000/2122/4230450/4230452/ISO_IEC_Directives_Part_1_and_Consolidated_ISO_Supplement_-_2014_%285th_edition%29_-_PDF.pdf?nodeid=16578881&vernum=-2 (6.10.2014).

[148] Der Begriff Deming-Kreis geht auf William Edwards Deming, 1900 – 1993 zurück, der als Pionier des Qualitätsmanagements gilt und als Grundlage aller QM-Systeme die Phasen eines kontinuierlichen Verbesserungsprozesses beschreibt.

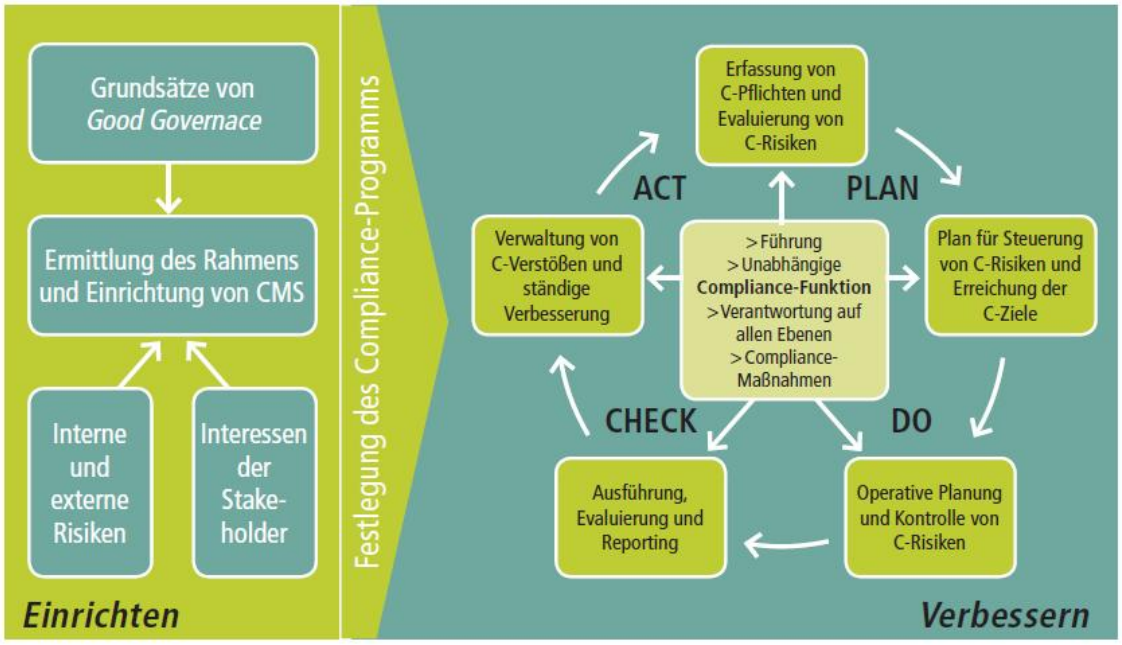

Abbildung 1: CMS nach ISO 19600[149]

Wie die oben gezeigte Abbildung zeigt, lässt sich die ISO 19600 in zwei wesentliche Abschnitte teilen – Schaffung der Voraussetzungen eines CMS nach ISO 19600 („Establish“) und kontinuierlicher Verbesserungsprozess („Improve“).

Hierbei ist natürlich zu berücksichtigen, dass die Schritte unter „Improve“ (Verbessern) selbstverständlich auch bei der erstmaligen Einrichtung zu beachten sind und erst im Rahmen der sukzessiven Wiederholung zu Verbesserungen führen.

(1) Schaffung der Voraussetzungen eines CMS nach ISO 19600 („Establish“ - Einrichten)

Das CMS nach ISO 19600 basiert auf den Prinzipien von „good governance“ sowie Flexibilität, Verhältnismäßigkeit Transparenz und Nachhaltigkeit. Nach einer kurzen Einführung unter anderem zum universalen Anwendungsbereich (Zif. 1) und Begriffsdefinitionen (Zif. 3) wird in Ziffer 4 der ISO 19600 die

[149] Makowicz, Compliance Praxis (Deutschland), 33ff. (34) – Eine vergleichbare Abbildung ist im ISO 19600 enthalten (Introduction, Seite V).

Organisation dazu angehalten, zunächst das relevante Compliance Umfeld der Organisation zu identifizieren. Im Rahmen der erstmaligen Einrichtung des CMS sind interne und externe Sachverhalte wie beispielsweise Compliance Risiken zu erfassen, die für den Zweck der Organisation relevant sind und das angestrebte Ziel des CMS beeinträchtigen können (Zif. 4.1). Weiters sind, die sogenannten „interested parties“[150] und deren Anforderungen zu bestimmen (Zif. 4.2).

Der individuellen Anwendungsbereichs des CMS in der jeweiligen Organisation ist zu definieren (Zif. 4.3) – also zum Beispiel die Frage ob es nur für bestimmte organisatorische Einheiten oder Teile einer Organisation eingeführt wird. Das CMS hat die sogenannten „good governance principles“ zu berücksichtigen (Zif. 4.4).[151] Hierzu gehören insbesondere die Grundsätze

- des direkten Zugangs des Compliance Verantwortlichen zum Aufsichtsorgan[152] der Organisation,
- der Unabhängigkeit der Compliance Verantwortlichen und
- der hinreichenden Befugnissen sowie
- ausreichender Ressourcen.

Hier wird bereits vorausgesetzt, was später als Teil des CMS vorgesehen wird: die Einrichtung einer unabhängigen Compliance Funktion (Zif. 5.3.1, 5.3.3, 5.3.4).

Die folgenden Zif. 4.5 und 4.6 sind die Schnittstellen in den Verbesserungsprozess, die sich in der Folge – wie auch die anderen Elemente des Verbesserungsprozesses – ständig wiederholen müssen. Im Wesentlichen

[150] „Interested parties“ oder Stakeholder werden in ISO 19600 definiert als Personen oder Organisationen, die eine Entscheidung oder Aktivität beeinflussen können oder hierdurch beinflusst werden können oder meinen hierdurch beeinflusst zu werden („person or organization (3.01) that can affect, be affected by, or perceive themselves to be affected by a decision or activity”).

[151] Auch hier wird entsprechend auf den PDCA Zyklus referenziert – Einrichtung, Entwicklung, Implementierung, Evaluierung, Wahrung und Verbesserung.

[152] Als Aufsichtsorgan wird hier der sogenannte „governing body“ bezeichnet, also dem Organ, dem die oberste Leitung der Organisation Rechenschaft zu legen hat – in einer Kaptitalgesellschaft also die Gesellschafterversammlung oder der Aufsichtsrat respektive der Verwaltungsrat)– ISO 19600 definiert hier wie folgt: „person or group of people that governs an organization (3.01), sets directions, and holds top management (3.05) to account“.

wird hier die systematische Identifizierung und Erfassung der verpflichtenden und freiwilligen Compliance Vorgaben gefordert. (Zif. 4.5.1). Im Rahmen einer entsprechenden Pflege sind diese Vorgaben regelmäßig zu überprüfen (Zif. 4.5.2). In Zif. 4.6 werden Grundsätze der Risiko-Identifizierung, Analyse und Bewertung genannt. Ein Verweis auf die ISO 31000[153] zeigt, wie sehr sich ein CMS nach ISO 19600 an Risiko Management Prozessen orientiert.

Sowohl für die Erfassung als auch für die Identifizierung, Analyse und Bewertung werden keine Vorgaben gemacht. Diese können daher im Rahmen der jeweiligen Verhältnismäßigkeit an die jeweilige Organisation angepasst werden.

(2) Kontinuierlicher Verbesserungsprozess („Improve“ - Verbessern)

Der kontinuierliche Verbesserungsprozess ist nur möglich, wenn wesentliche zentrale CMS Elemente geschaffen werden.

(a) Zentrale Elemente

Im Zentrum des Verbesserungsprozesses des CMS nach ISO 19600 stehen die Führung und die unzweifelhafte Aussage der Führung (hier Aufsichtsorgan und die oberste geschäftsverantwortliche Leitung der Organisation, das Top Management[154]) zur Bedeutung des jeweiligen CMS für die Organisation (Zif. 5.1). – also der klare „Tone from the top“ – sowie die Unabhängigkeit des Compliance Verantwortlichen. Dies wird auch im Kapitel „Bewusstsein“ in Zif. 7.3.3.2 hervorgehoben, wo die Schlüsselverantwortung und –bedeutung des Top Managements für die effektive Umsetzung von Compliance nochmals herausgestellt wird.

[153] ISO/IEC 31000:2009 Risk Management – Guidelines for principles and implementation of risk management.

[154] ISO 19600 definiert „top management“ als “person or group of people who directs and controls an organization (3.01) at the highest level” - in einer Kapitalgesellschaft also die Geschäftsführung oder der Vorstand bzw. der/die geschäftsführende(n) Direktor(en).

Es ist eine individuelle Compliance-Policy zu entwickeln, die die wesentlichen Compliance-Leitlinien enthält (Zif. 5.2). Zif. 5.3.1 sieht vor, dass Funktionen und Zuständigkeiten des „Top Managements“ im Hinblick auf die Compliance Verantwortlichkeiten klar zu bestimmen sind. Gem. Zif. 5.3.2 kann abhängig von der individuellen Organisation eine Person als Compliance Verantwortlicher bestimmt werden oder die Aufgaben können durch ein „cross-funktionales“ Team wahrgenommen werden. Den Verantwortlichen sind gem. Zif. 5.3.3 durch die Organisationsleitung und das Top Management alle Ressourcen und Zugänge – insbesondere zu den Entscheidungsträgern, allen Ebenen der Organisation, allen notwendigen Informationen und notwendigen Experten - zur Verfügung zu stellen, um den Anforderungen der ISO 19600 gerecht zu werden und ein wirksames CMS zu schaffen und zu bewahren.

Zif. 5.3.4 und 5.3.5 fassen die Aufgaben des Compliance Verantwortlichen sowie des Managements (keine Eingrenzung auf Top Management) zusammen. Insbesondere Ziffer 5.3.4 kann hier im Sinne einer Job Description für einen Compliance Verantwortlichen gesehen werden. Den Mitarbeitern der Organisation werden in 5.3.5 zuletzt die Aufgaben zugewiesen, die für sie relevanten Compliance Vorschriften einzuhalten, an Compliance Trainings teilzunehmen und entsprechend zu berichten, sofern Compliance betroffen ist oder betroffen sein kann. Alle Aktivitäten im Zusammenhang mit dem notwendigen Compliance Kompetenz Management und Training sind zentral in Zif. 7.2 enthalten.

Wie bereits auch schon unter den sogenannten „good governance principles“ genannt,[155] ist hier als weiteres zentrales Element die erforderliche Absicherung der notwendigen Unterstützung des kontinuierlichen Verbesserungsprozesses durch Vorhalten der notwendigen Ressourcen zu nennen (Zif. 7.1).

Zuletzt sind in Zif. 7.3 die Bewusstseinsbildung in der Organisation zum Thema Compliance sowie die Erforderlichkeit und Details im Zusammenhang mit einem

[155] s.o. S. 55.

Compliance Kommunikationsplanes (Zif. 7.4) sowie der notwendigen Compliance Dokumentation (Zif. 7.5) dargestellt.

(b) Develop – Implement – Evaluate – Maintain (PDCA Zyklus)

Auf Basis der Ergebnisse der Aktivitäten zur Schaffung der Voraussetzungen eines CMS nach ISO 19600[156] sind die zur Adressierung der identifizierten Compliance Risiken erforderlichen Compliance Maßnahmen und Compliance Ziele zu planen (Zif. 6). Insbesondere ist hierbei zu berücksichtigen, dass die Umsetzung der Ziele messbar ist und die Maßnahmen in die Geschäftsprozesse implementiert und effektiv umgesetzt werden können.

Die operative Umsetzung der entwickelten Maßnahmen kann gem. Zif. 8 entweder durch die eigenen Ressourcen der Organisation selbst oder durch entsprechende Delegation an Dritte (outsourced processes). Effektive Kontrollen zur Absicherung der Einhaltung der Compliance Verpflichtungen der Organisation sind ein- und regelmäßig durchzuführen.

Zur Absicherung des Verbesserungsprozesses hat entsprechend der Vorschläge in Zif. 9 eine Planung zu erfolgen, was im Rahmen des CMS einer kontinuierlichen Überwachung durch entsprechende Compliance Kontrollen und Messung unterliegt. Diese Planung ist in der Folge umzusetzen. Feedbacks sind bei geeigneten Stellen einzuholen, Informationen zu sammeln. Neben anderen Quellen werden hier die Einrichtung von sogenannten Whistleblowing Systemen (Hinweisgebersysteme) oder eigene Ermittlungen empfohlen. ISO 19600 betont in Zif. 9.1.6 die Bedeutung der Entwicklung und Anwendung von messbaren Indikatoren, um die Zielerreichung und die Compliance Leistung messen zu können. Sodann wird eine Berichterstattung und die Archivierung der im Zusammenhang mit Compliance relevanten Unterlagen vorgesehen.

[156] ebenda.

Als wesentliches Element des Verbesserungszyklus werden in Zif. 9.2 regelmäßige Audits durch die Organisation sowie in Zif. 9.3 Bewertungen („reviews“) durch das Top Management vorgesehen.

Zuletzt wird unter Ziffer 10 (Improvement) behandelt, wie bei Nichteinhaltung der Anforderungen des jeweiligen CMS (noncoformity) und bei Compliance Verstößen (noncompliance) vorzugehen ist. Um den Informationsfluss abzusichern, wird für solche Fälle vorgeschlagen, einen Eskalationsprozess einzuführen. Ständig solle die Organisation danach streben, die Eignung, Verhältnismäßigkeit und die Wirksamkeit des CMS zu steigern.

Im Sinne der kontinuierlichen Verbesserung sind entsprechend der Ziffer 4.5f.[157] konsequent die verpflichtenden und freiwilligen Compliance Vorgaben zu aktualisieren und der Compliance Prozess ständig zu leben.

b) *TR CMS 101:2011*

Vom TÜV Rheinland wurde der Standard für Compliance Management Systems des TÜV Rheinland - TR CMS 101:2011 entwickelt. Zur Interpretation und Erläuterung dieses Standards dient der Compliance Leitfaden TR CMS 100:2013 des TÜV Rheinland.

aa) TÜV Rheinland

Als Prüfdienstleister und Berater für technische Anlagen, Produkte und Dienstleistungen, Projekte und Prozesse[158] nutzt der TÜV Rheinland den Standard TR CMS 101:2011 bei der Prüfung und Zertifizierung von CMS. Nach eigenen Angaben ist der TÜV Rheinland ein international führender Dienstleistungskonzern dessen Marke für Sicherheit, Effizienz und Qualität von

[157] s.o. S. 55.
[158] http://www.tuv.com/media/germany/60_systeme/csr_nachhaltigkeit_compliance/compliance/faktenblaetter/Whitepaper_Compliance.pdf (29.07.2014).

Mensch, Umwelt und Technik steht.[159] Unter anderem prüft, begleitet, entwickelt, fördert und zertifiziert der TÜV Rheinland als neutraler, unabhängiger Dritter Produkte, Anlagen, Prozesse und Managementsysteme sowie Dienstleistungen auf Basis gesetzlicher Vorgaben und weiterer relevanter Leistungsmaßstäbe und Standards.[160] Auch wenn die Ursprünge und die Basis des TÜV Rheinland wohl unzweifelhaft technischer Natur ist, bietet TÜV Rheinland heute Dienstleistungen für eine Vielzahl von Wirtschaftszweigen und Lebensbereichen an.[161]

bb) Allgemein zum Standard TR CMS 101:2011

Der Standard legt die Anforderungen an ein CMS nach TR CMS 101:2011 fest. Wie im Compliance Leitfaden TR CMS 100:2013 erläutert wird, sind die Anforderungen des TR CMS 101:2011 generisch und allgemeiner Natur und können auf alle Organisationen – unabhängig von Art und Größe, Standort oder Art des Geschäfts angewandt werden. Aufgrund der internationalen Ausrichtung gibt es den Standard in deutscher und englischer Sprache.[162]

Vergleicht man den Standard TR CMS 101:2011 mit ISO 19600, so fällt zunächst auf, dass der Standard TR CMS 101:2011 wesentlich kürzer ist. Ein Grund hierfür ist sicher, dass ISO 19600 inhaltlich sehr detailliert ist und als Leitfaden weitreichende Vorschläge für ein effektives CMS darstellen kann. Auch sind die Erläuterungen zum Standard in einem anderen Dokument (TR CMS 100:2013) enthalten, so dass TR CMS 101:2011 kürzer ausfallen kann.

cc) Adressat des Standards TR CMS 101:2011

Der Standard soll nach Angaben des TÜV Rheinland für alle Organisationen geeignet sein, die sich ein Bild darüber machen wollen, ob sie über ein

---

159 http://www.tuv.com/de/deutschland/ueber_uns/kompetenzen/kompetenzen.html (21.08.2014).

160 http://www.tuv.com/de/deutschland/ueber_uns/kompetenzen/leistungen/leistungen.html (21.08.2014).

161 http://de.wikipedia.org/wiki/T%C3%9CV_Rheinland (21.08.2014).

162 TR CMS 100:2013, A.1.2 – 1.5.

wirksames Compliance Management Systems verfügen. Dies gelte sowohl für mittelständische Unternehmen als auch für Großunternehmen bzw. internationale Konzerne.[163] Im Unterschied zu IDW PS 980, der die Prüfung eines CMS beschreibt,[164] ist sowohl im TR CMS 101:2011 als auch im TR CMS 100:2013 nicht die Prüfung und damit der Prüfer im Vordergrund, sondern das CMS selbst und die Beschreibung des Managementsystems an sich.

Wie sich aus der Verwendung von Begrifflichkeiten wie „Organisation“ und „Oberste Leitung“ ableiten lässt und auch aus dem Compliance Leitfaden TR CMS 100:2013 ergibt, weist der CMS Standard eine große Kompatibilität zum QM-System nach ISO 9001 auf.[165] Diese Übereinstimmungen werden auch bei einem Vergleich der Standardanforderungen deutlich.[166] Der TÜV Rheinland hat sich deutlich von der ISO 9001 leiten lassen und sich weitgehend an der Gliederung dieser Norm orientiert. TR CMS 101:2011 folgt damit dem gleichen Ansatz wie ISO 19600, enthält aber noch nicht die High Level Structure die erst in der nächsten Version der ISO 9001 in diese Norm implementiert werden soll.[167]

Aufgrund der gewollten Kompatibilität des Standards mit QM-Systemen nach ISO 9001 ist der Standard insbesondere an Organisationen – und damit auch Industrieunternehmen – gerichtet, die bereits über ein nach ISO 9001 zertifizierten QM-System verfügen.

---

[163] http://www.tuv.com/de/deutschland/gk/managementsysteme/nachhaltigkeit_csr/compliance_management/compliance_management.html (29.07.2014).
[164] siehe unten S. 67ff.
[165] Die Begriffe „Organisation“ und „Oberste Leitung“ sind in de ISO 9000 definiert, auf die auf die ISO 9001 verweist. Es fällt jedoch auf, dass die Begriffe und das Ziel der Kompatibilität zwar vorhanden sind, die Definitionen aber nicht. So wird die oberste Leitung in Ziff. 3.2.7 der ISO 9000:2005 definiert als „Person oder Personengruppe, die eine Organisation auf der obersten Ebene leitet und lenkt“. Der TR CMS 100:2013 definiert die Oberste Leitung als „Unternehmensleitung, Geschäftsführung“. Ebenfalls wird der Begriff „Organisation“ in der ISO 9000:2005 definiert, als „Gruppe von Personen und Einrichtungen mit einem Gefüge von Verantwortungen, Befugnissen und Beziehungen“. TR CMS 100:2013 definiert diesen Begriff als „Unternehmen, Betrieb, Firma. […]“.
[166] siehe unten unter dd) Grundelemente eine CMS nach TR CMS 101:2011.
[167] http://www.iso.org/iso/iso9001_revision (08.01.2015).

dd) Grundelemente eine CMS nach TR CMS 101:2011

Nach allgemeinen Erläuterungen (Zweck des CMS, Anwendungsbereich, Ziele und Begriffe) werden die Standardanforderungen an ein CMS beschrieben.[168]

Nicht zu verwechseln sind diese Standardanforderungen mit den Grundsätzen, die ein CMS nach TR CMS 101:2011 zu berücksichtigen hat.[169] Die Standardanforderungen sind in Kapitel 4 – 8 beschrieben.

Entsprechend folgt das CMS ebenfalls dem PDCA-Zyklus.[170]

In konsequenter Fortführung des PDCA-Zyklusses basieren auch die Grundelemente des CMS nach TR CMS 101:2011 auf dem Gedanken des kontinuierlichen Verbesserungsprozesses.

[168] TR CMS 101:2011, 4. – 8.
[169] TR CMS 100:2013, A.3: Hierzu zählen die Themen Compliance Kultur, Führung, Einbeziehung der Mitarbeiter, Administration des Compliance-Systems durch einen Compliance-Beauftragten, Compliance Risikoanalyse, Systemorientierter Managementansatz, Systemüberwachung, -analyse und –verbesserung.
[170] siehe auch TR CMS 100:2013, a.2.

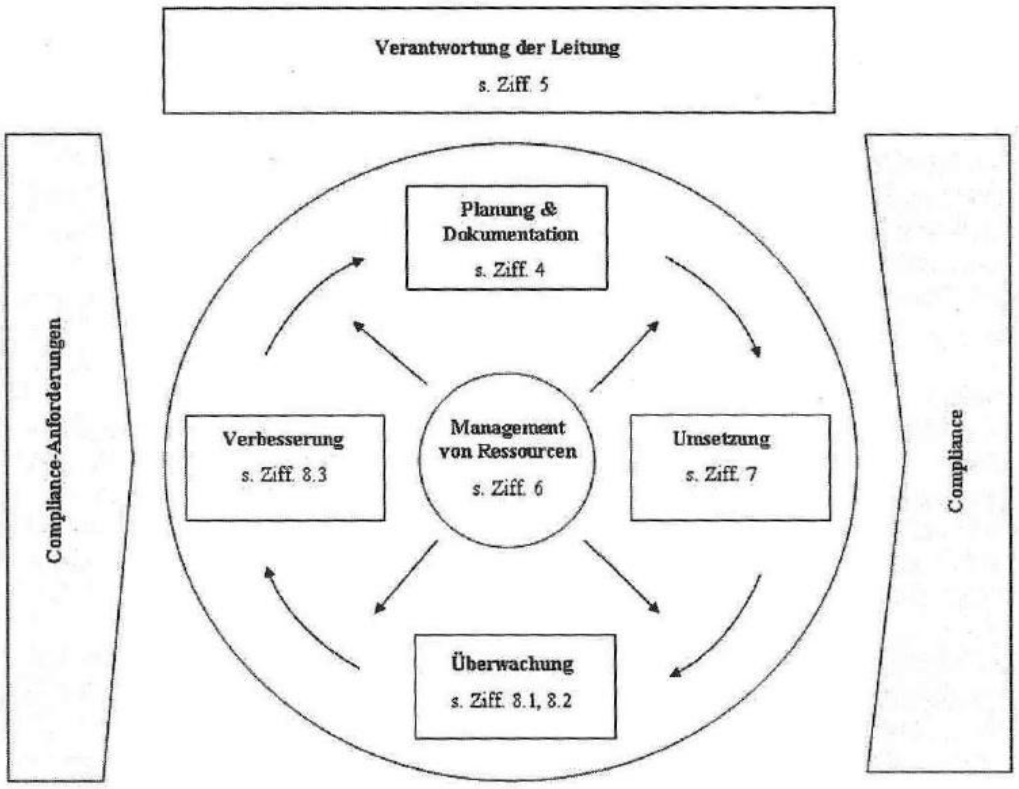

Abbildung 2: Modell eines prozessorientierten Compliance Management Systems (CMS) nach TR CMS 101:2011[171]

Genannt werden in Kapitel 4 die allgemeinen und Dokumentationsanforderungen an ein CMS sowie die Lenkung von Vorgabe[172]- und Nachweisdokumenten.

Es folgen im Kapitel 5 Anforderungen an die Verantwortung der Leitung für einen klaren „Tone from the Top“ und die Funktionsfähigkeit des CMS, das in regelmäßigen Abständen zu bewerten ist. Es ist ein Compliance-Beauftragter zu benennen und mit den erforderlichen Befugnissen auszustatten sowie die Compliance Kommunikation sicherzustellen.

[171] TR CMS 101:2011, S. 4.
[172] als Beispiele für Vorgabedokumente werden in TR CMS 100:2013, B. unter anderem Rechts- und Genehmigungskataster, Freigabeverfahren und Prüfpläne, etc. genannt.

Kapitel 6 betrifft das Ressourcenmanagement im Hinblick auf die Verfügbarkeit ausreichend geschulten und erfahrenen Personals zum Thema Compliance sowie der erforderlichen Infrastruktur. Wesentlich ist, dass hier keine quantitativen Vorgaben gemacht werden. Es wird lediglich gefordert, dass die Organisation die erforderlichen Ressourcen ermittelt und bereitstellt, um das CMS zu verwirklichen, aufrechtzuerhalten und laufend zu verbessern.

In Kapitel 7 wird zum Thema der Compliance-Prozesse und deren Umsetzung ein stufenweises Vorgehen vorgegeben. Nach Identifizierung der spezifischen Compliance-Risiken und Compliance-Vorgaben in der Organisation wird die Definition der jeweils angemessenen Maßnahmen gefordert, die in die Arbeitsprozesse integriert werden müssen. Interessenskonflikte sind zu vermeiden („Segregation of duties“), Freigabe-/Genehmigungsprozesse zu definieren. Jeder muss über die Möglichkeit verfügen, anonyme Hinweise zu geben („whistleblowing“) oder Beratung zu bekommen. Zuletzt wird hier ein dokumentiertes Verfahren zum Umgang mit Compliance-relevanten Vorgängen gefordert.

Das letzte Kapitel 8 betrifft die Systemüberwachung, -analyse und –verbesserung durch interne Audits und geeignete Überwachungsmethoden. Dies bedeutet, dass auch Compliance-Funktionen einer Überprüfung durch Auditierung unterliegen müssen und die Effektivität der Funktionen beispielsweise durch KPI’s zu messen ist. Ziel ist immer die ständige Verbesserung die durch Korrektur- und Vorbeugemaßnahmen anzustreben ist.

c) ***ONR 192050:2013 02 01***[173]

Die ON-Regel "Compliance Managementsysteme - Anforderungen und Anleitung zur Anwendung" (ONR 192050) von Austrian Standards, ist ein von Vertretern der Wirtschaft in einem vom Austrian Standards Institute einberufenen Expertenkomitee ausgearbeiteter Standard für CMS.

[173] im Folgenden ONR 192050.

aa) Austrian Standards Institute

Das Austrian Standards Institute ist eine in Österreich als Verein eingetragene Plattform[174], die für die Schaffung von österreichischen Normen und für die Umsetzung von EU-Normen in Österreich zuständig ist. Sie ist im Jahre 2009 aus dem Österreichischen Normungsinstitut hervorgegangen. Rechtliche Basis für diese Tätigkeit ist § 1 Normengesetz 1971.

bb) Allgemein zur ONR 192050

ON-Regeln sind normative Dokumente, die nicht alle Anforderungen an eine "klassische" Norm“ erfüllen müssen. Sie ist ebenso wie die klassische Norm ein standardisiertes Regelwerk und das österreichische Gegenstück zu "Workshop Agreements" (CEN, ISO) und "Publicly Available Specifications" (ISO), die sich auf europäischer und internationaler Ebene etabliert haben. Ihre Anwendung ist – ebenso wie bei den Normen – nicht verpflichtend.[175]

Nach einem Vorwort und Begriffserläuterungen folgen 2,5 Seiten zu den Anforderungen an ein CMS. Eine Kommentierung ist nicht enthalten.[176]

cc) Adressat

Die ONR 192050 wendet sich an alle Organisationsformen und Organisationsgrößen. Die ONR 192050 wurde maßgeblich von Vertretern der Wirtschaft in einem vom Austrian Standards Institute einberufenen Expertenkomitee (Komitee 265 „Compliance Systeme“) von Vertretern

[174] ZVR-Zahl 627457584.
[175] Petsche-Toifl-Neiger-Jirges, S. 13; siehe auch allgemein zum Ziel der Normung VERORDNUNG (EU) Nr. 1025/2012 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 25. Oktober 2012 zur europäischen Normung, Beweggrund (1): „Das Hauptziel von Normung ist die Festlegung freiwilliger technischer oder die Qualität betreffender Spezifikationen, denen bereits bestehende oder künftige Produkte, Produktionsverfahren oder Dienstleistungen entsprechen können.“
[176] Eine Kommentierung wird jedoch in Form eines 156 seitigen Praxiskommentars über die Austrian Standards plus GmbH vertrieben (Petsche-Toifl-Neiger-Jirges, Compliance Management Systems (CMS) – die ONR 192050 – weitere Angaben hierzu im Literaturverzeichnis).

verschiedener Wirtschaftszweige, Rechtsanwälten und Sachverständigen ausgearbeitet und mehrheitlich verabschiedet.[177] Auch aus diesem Grunde wird sie als besonders praxisorientiert bezeichnet.[178]

Sie erhebt den Anspruch, insbesondere auch für KMUs geeignet zu sein, da sie nicht den Aufbau personeller Ressourcen fordere, sondern lediglich Rollen definiere.[179] Auch ist zu lesen, dass andere CMS Standards wie der IDW PS 980 extensive und detaillierte Dokumentationspflichten unabhängig von der jeweiligen Organisationsform und –größe normiere. Kleinere Organisationen hätten es daher ungleich schwerer als große Organisationen eine CMS Zertifizierung zu erlangen, als dies bei der Zertifizierung nach ONR 192050 der Fall sei.[180]

dd) Grundelemente eines CMS nach ONR 192050

ONR 192050 beschreibt in Ziffer 3 - 9 das CMS. Die ONR definiert in Ziffer 3 nach einem Leitsatz zunächst die Anforderungen an das Verhalten der Leitung der jeweiligen Organisation. Wesentlich ist auch hier, dass die Leitung neben dem eigenen Verhalten als Vorbild für die Ausrichtung der gesamten Organisation zuständig ist.

Im folgenden Kapitel 4 werden die Rolle und Aufgaben des Compliance Officers beschrieben. Die weisungsunabhängig auszugestaltende Rolle des Compliance Officers kann entweder von einem Leitungsmitglied oder einem oder mehreren Organisationsmitgliedern wahrgenommen werden kann.

Danach werden in Ziffer 5 die Rahmenbedingungen für das Verfahren der Compliance-Risiko-Bewertung und die daraus abzuleitenden Compliance Maßnahmen erläutert.

[177] ONR 192050, Vorwort, S. 3; Petsche-Toifl-Neiger-Jirges, S. 9.
[178] Petsche-Toifl-Neiger-Jirges, S. 9.
[179] ONR 192050, Vorwort, S. 3; Petsche/Trafoier weisen in Compliance Praxis 2013, S. 6ff (Heft 1) darauf hin, dass Vertreter von KMUs im Komitee 265 „Compliance Systeme“ beteiligt waren.
[180] Petsche/Trafoier, Compliance Praxis 2013, S. 6 ff. (Heft 1).

Anschließend wird in Ziffer 6 vorgesehen, dass aus der Compliance-Risiko-Bewertung abgeleitete und verbindliche Handlungsanweisungen dokumentiert werden und Schlüsselpositionen im Unternehmen nur mit Kandidaten besetzt werden, die unter Compliance-Gesichtspunkten überprüft wurden.

Im Hinblick auf die jeweiligen Aufgaben der Organisationsmitglieder angepasste und dokumentierte Compliance Trainings sind nach Ziffer 7 ein wesentlicher Teil eines CMS nach ONR 192050.

Die Einhaltung der Handlungsanweisungen ist entsprechend der folgenden Ziffer 8 ebenso zu überwachen wie auch compliance-relevante Vorgaben zu überprüfen sind. Ebenfalls sind die Angemessenheit, Eignung und Wirksamkeit des CMS regelmäßig zu überprüfen. Whistleblowing muss auch anonym möglich sein. Entsprechend den dafür festgelegten Verfahren sind Regel-Verstöße zu sanktionieren.

Zuletzt wird in Ziffer 9 die Verpflichtung zu einer regelmäßigen Kommunikation des Engagements für Compliance durch die Leitung im Sinne eines „tone from the top“ und die Information der Organisation über Änderungen vorgesehen.

d) ***IDW PS 980***

Das deutsche Institut der Wirtschaftsprüfer hat am 11.03.2011 den Prüfungsstandard „Grundsätze der ordnungsgemäßen Prüfung von Compliance Management Systemen (IDW PS 980)“ verabschiedet.

aa) Institut der Wirtschaftsprüfer

Das „Institut der Wirtschaftsprüfer in Deutschland e.V.“ ist ein eingetragener Verein und vereint Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften in Deutschland auf freiwilliger Basis. Nicht zu verwechseln ist der IDW mit der Wirtschaftsprüferkammer. Satzungsgemäße Aufgabe des IDW ist es unter

anderem für einheitliche Grundsätze der unabhängigen, eigenverantwortlichen und gewissenhaften Berufsausübung einzutreten und deren Einhaltung durch die Mitglieder sicherzustellen.[181]

bb) Allgemein zum Prüfungsstandard

Die IDW Prüfungsstandards legen die Berufsauffassung der Wirtschaftsprüfer zu fachlichen Fragen der Prüfung dar und tragen zu ihrer Entwicklung bei. Im IDW PS 201, Tz. 28 und 29 wird die Bedeutung der IDW PS beschrieben. Danach handelt es sich um Grundsätze zur ordnungsgemäßen Durchführung von Abschlussprüfungen sowie Festlegungen zu den dabei vorzunehmenden Prüfungshandlungen. Abweichungen von den IDW Prüfungsstandards können im Rahmen der Eigenverantwortlichkeit des Wirtschaftsprüfers nur in Ausnahmefällen erfolgen Werden die IDW Prüfungsstandards vom Abschlussprüfer nicht beachtet, wird auf ein Regressrisiko, ein mögliches Verfahren der Berufsaufsicht oder ein nicht auszuschließendes Strafverfahren zum Nachteil des Abschlussprüfers hingewiesen.[182]

Nicht anwendbar ist der Prüfungsstandard dort, wo entweder sogenannte „agreed upon procedures“ mit dem Wirtschaftsprüfer vereinbart werden, oder Prüfungen durchgeführt werden, für die spezielle Prüfungsstandards bestehen.[183] Vor dem 30.09.2011 war die Anwendung des Prüfungsstandards freiwillig.[184]

---

[181] siehe unter http://www.idw.de/idw/portal/n281334/n379162/index.jsp (29.07.2014); SATZUNG DES INSTITUTS DER WIRTSCHAFTSPRÜFER IN DEUTSCHLAND E. V., in der Fassung der auf dem 27. Wirtschaftsprüfertag am 19. September 2005 in Neuss beschlossenen Satzungsänderung, siehe unter http://www.idw.de/books/IDW_Satzung_dt/files/assets/common/downloads/publication.pdf (13.01.2015).

[182] Auszug aus IDW WP-Handbuch 2012, S. 3011 unter: http://www.idw.de/idw/download/Download_Auszug_Anhang3_WPH2012.pdf?id=399948&property=Datei (29.07.2014) mit Verweis auf IDW PS 201, Tz. 28 und 29.

[183] IDW PS 980, Tz. 2, A1.

[184] IDW PS 980, Tz. 3 – wobei zu beachten ist, dass die CMS Prüfung nach deutschem und österreichischem Recht ohnehin freiwillig ist.

Der Prüfungsstandard IDW PS 980 ist ein in sich geschlossenes Dokument, das nach allgemeinen Erläuterungen und Begriffsbestimmungen Informationen zu Gegenstand, Ziel und Umfang der Prüfung eines CMS gibt und die wesentlichen Grundelemente eines CMS kurz aufzählt und erklärt. Nach weiteren Aussagen zu Prüfungsanforderungen (zB Berufspflichten, Auftragsannahme, Prüfungsplanung und –durchführung) folgen Hinweise zum Prüfungsurteil und Aufbau bzw. Inhalt des Prüfungsberichts. Einen umfangreichen Teil nehmen die Anwendungshinweise und Erläuterungen zu den Grundelementen des CMS und der Prüfung sowie Textvorlagen für Feststellungen und Empfehlungen des Prüfers ein.

cc) Adressat des Prüfungsstandards

Der Prüfungsstandard richtet sich zunächst nur an Wirtschaftsprüfer. Er enthält nach Vorbemerkungen und Begriffsbestimmungen (Tz. 1 – 11) zunächst Hinweise, was Gegenstand der Prüfung ist, wie die Prüfung eines CMS stattzufinden hat und was der Prüfer bei der Prüfung zu beachten hat. Er beschreibt daher im Wesentlichen – gemessen am Umfang – nicht das CMS selbst, sondern stellt eine Prüfanweisung für die Prüfung von CMS durch einen Wirtschaftsprüfer dar. Dies schließt jedoch nicht aus, dass auch andere Institutionen, Berater oder Rechtsanwälte eine Prüfung nach IDW PS 980 vornehmen können. Eine Bindungswirkung entfaltet er jedoch nur für den Berufsstand der Wirtschaftsprüfer.[185]

Der Prüfungsstandard weist darauf hin, dass er lediglich den Inhalt freiwilliger CMS Prüfungen verdeutlicht.[186] Eine solche Prüfung wäre damit im Rahmen einer Erweiterung des gesetzlichen Prüfungsauftrags oder einer Stand-alone Prüfung vertraglich zu vereinbaren. Man könnte annehmen, dass solche Vereinbarungen im Wesentlichen mit mittleren und großen Kapitalunternehmen

[185] Berndt, BB 2012(14),VI – VII – hier ist aber zu berücksichtigen, dass der IDW lediglich ein privatwirtschaftlicher Verein ohne öffentlich-rechtliche Befugnisse ist. Nichtsdestotrotz geht von den IDW PS wohl zumindest handelsrechtlich eine faktische Bindungswirkung aus – siehe hierzu Schiel, S. 47ff., m.w.N.
[186] IDW PS 980, Tz. 1.

erfolgen, mit denen der Wirtschaftsprüfer ohnehin in Kontakt ist, da er den Jahresabschluss verpflichtend zu prüfen hat.[187]

Der IDW PS 980 kann neben der Prüfung von Unternehmen im engeren Sinn auch bei Prüfungen von anderen Organisationen (Vereine, Gesellschaften bürgerlichen Rechts, Gebietskörperschaften, Anstalten des öffentlichen Rechts oder anderen nicht rechtlich selbstständige wirtschaftliche Einheiten angewandt werden.[188]

Neben der Eigenschaft als Prüfungsstandard kann der IDW PS 980 – wie im Übrigen auch die anderen CMS Standards – als Anleitung für Unternehmen dienen, ein CMS einführen wollen.[189]

dd) Grundelemente eine CMS nach IDW PS 980

Ein CMS soll nach dem Prüfungsstandard IDW PS 980 aus sieben Grundelementen bestehen, die in Wechselwirkung zueinander stehen und sich gegenseitig beeinflussen: Compliance-Kultur, Compliance-Ziele, Compliance-Risiken, Compliance-Programm, Compliance-Organisation, Compliance-Kommunikation sowie Compliance-Überwachung und -Verbesserung.[190]

[187] So gibt auch Art. 34 I der EU Bilanzrichtlinie 2013/34/EU vor, dass die Mitgliedsstaaten vorzusehen haben, dass lediglich die Abschlüsse von Unternehmen von öffentlichem Interesse, mittleren und großen Unternehmen von zugelassenen Wirtschaftsprüfern zu prüfen sind - siehe auch für Deutschland §§ 316 I iVm 267 I HGB bzw für Österreich §§ 268 I UGB iVm 221 I UGB. Kleine Kapitalgesellschaften sind nach der österreichischen und der deutschen Regelung danach solche, die mindestens zwei der drei nachstehenden Merkmale nicht überschreiten
1. 4 840 000 Euro Bilanzsumme
2. 9 680 000 Euro Umsatzerlöse in den zwölf Monaten vor dem Abschlußstichtag
3. im Jahresdurchschnitt fünfzig Arbeitnehmer.

[188] IDW PS 980, Tz. 1, Fn. 2.

[189] Görtz, BB 2012, 178ff (179).

[190] IDW PS 980, Tz. 23, A14ff.

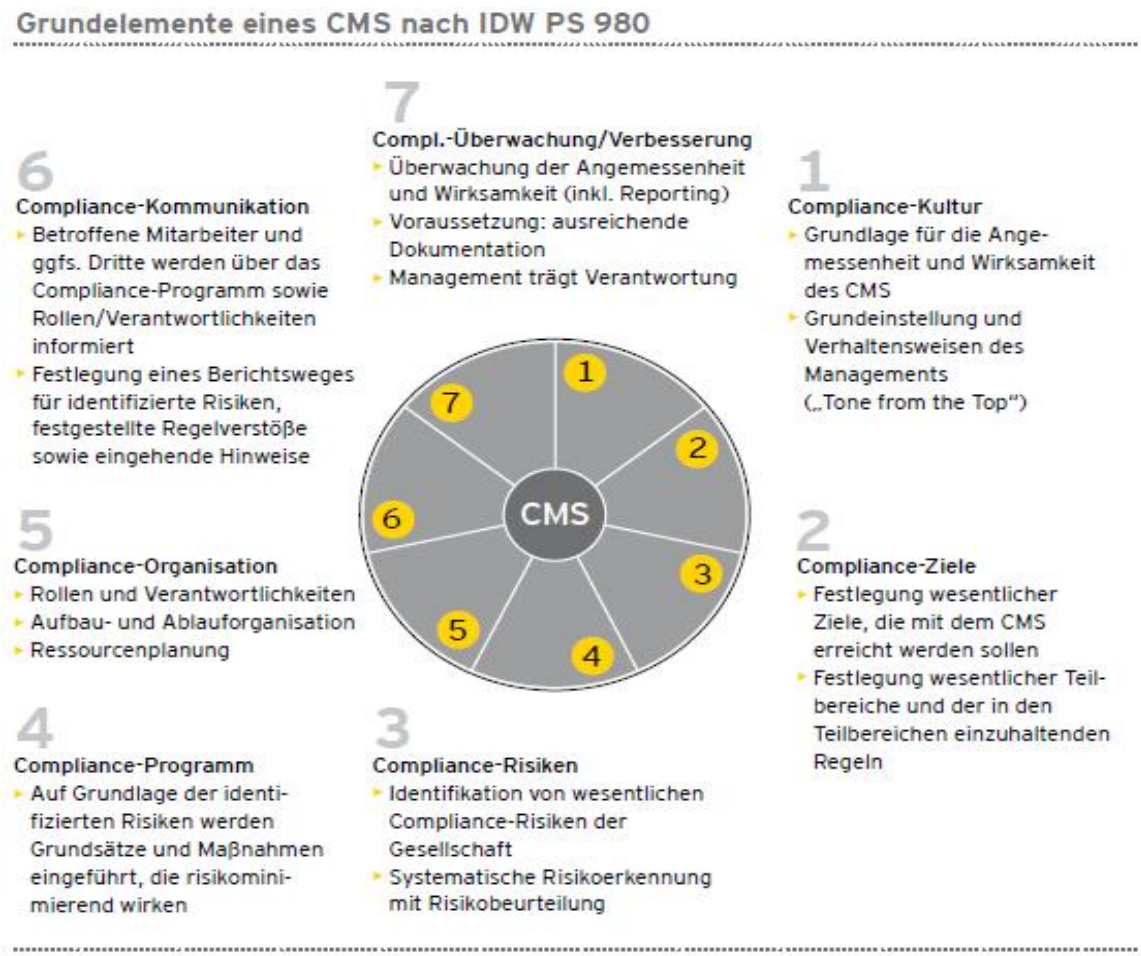

Abbildung 3: Grundelemente eines CMS nach IDW PS 980[191]

Die Compliance-Kultur im Unternehmen ist danach die Grundlage für das gesamte CMS. Die Compliance-Ziele sind für die jeweiligen Teilbereiche von der Leitung festzulegen und bilden die Grundlage für die Beurteilung der Compliance-Risiken. Diese Risiken sind systematisch zu identifizieren und zu berichten. Mit dem Ziel der Begrenzung der Compliance-Risiken und der Vermeidung von Compliance Verstößen sind im Rahmen des Compliance-Programms Grundsätze und Maßnahmen einzuführen. Als integraler Bestandteil der Unternehmensorganisation sind die Rollen und Verantwortlichkeiten der Compliance-Organisation festzulegen. Unter der Überschrift Compliance-Kommunikation sind Mitarbeiter und ggf. Dritte zu

[191] Abbildung 1 aus "Der IDW PS 980 Standard zur Prüfung von Compliance-Management-Systemen", 2011 Ernst & Young GmbH Wirtschaftsprüfungsgesellschaft, http://www.ey.com/Publication/vwLUAssets/EY_Flyer_zu_IDW_PS_980/$FILE/EY%20Flyer_IDW%20PS%20980.pdf (29.07.2014).

informieren und die Compliance-Berichterstattung durchzuführen. Zuletzt ist im Rahmen von Compliance-Überwachung und –Verbesserung das CMS zu kontrollieren, Verstöße zu berichten und das System zu verbessern.

Die im ersten Teil des IDW PS 980 auf etwas mehr als einer Seite dargestellten Grundelemente werden im zweiten Teil kurz erläutert.[192] Der Prüfer – aber auch das Unternehmen – kann anhand dessen das jeweilige System spiegeln. Anhand von Merkmalen und Beispielen werden die Grundelemente erklärt und Prozesse dargestellt.

2. Prüfung und Zertifizierung

Ein CMS kann sowohl durch interne aber auch durch externe Auditoren überprüft werden. Als interne Auditoren kommen im Regelfall die interne Revision in Betracht, als externe Prüfer Anwaltskanzleien, Wirtschaftsprüfer sowie im Bereich Compliance erfahrene Experten.

Alle erwähnten Standards empfehlen bzw. setzen die Überwachung des CMS durch prozessunabhängige Stellen voraus.[193] Die Überprüfung des CMS durch Compliance Verantwortliche selbst ist damit formal ausgeschlossen. Dies bedeutet aber nicht, dass Compliance Verantwortliche von Selbstüberprüfungen freigestellt wären. Im Rahmen von regelmäßigen Self Assessments zur Überprüfung der Wirksamkeit des CMS, zur Prüfungsvorbereitung und zur Identifizierung von Verbesserungspotentialen sind diese selbstverständlich ebenfalls möglich und nötig.

[192] IDW PS 980, Tz. A14ff.
[193] IDW PS 980, Tz. 23, A20; ISO 19600, Zif. 9.2, 10.2; ONR 192050, Zif. 8; TR CMS 101:2011, Zif. 8.1, 8.3.

Wesentliches Ziel der vollumfänglichen Prüfung ist

- die Sicherstellung der Umsetzung und Einhaltung der Anforderungen des jeweiligen Standards[194] und der individuellen Anforderungen des CMS sowie
- die Klärung, ob das CMS effektiv ist und damit auch die Verbesserung des CMS durch Auffinden von (möglichen) Schwachstellen[195].

Hierbei ist zu berücksichtigen, dass bei der Prüfung zunächst nur das CMS selbst überprüft wird, nicht jedoch individuelle Compliance Risiken und die Frage, ob die Organisation sich selbst compliant verhält.[196] Das Gleiche gilt für Zertifizierungsaudits.[197] Insofern ist die Prüfung nicht mit den sogenannten Compliance Kontrollen zu verwechseln. Diese gehören zu den Compliance Maßnahmen und dienen der Verhinderung des Eintritts von Compliance Risiken selbst.

Wesentlich bei jeder Prüfung ist aber die Dokumentation aller Details des CMS und der im Rahmen des CMS implementierten Compliance Maßnahmen. Nur wenn dies sichergestellt ist, kann die Implementierung und Effektivität des CMS dem Prüfer (oder auch dem Richter im gerichtlichen Verfahren) nachgewiesen werden.

Die Praxis zeigt, dass bei der Einführung eines CMS die Kosten des Systems und der aus ihm folgenden Maßnahmen oft hoch sind. Ein Grund hierfür ist sicherlich, dass das CMS oftmals aufgrund eines Anlassfalles eingeführt wird, der zu einem Druck von außen – beispielsweise durch ein laufendes Straf- oder Bußgeldverfahren – geführt hat. In diesen Fällen stehen bei der Einführung die Verhinderung der individuellen Compliance Risiken zunächst gegenüber den Kosten im Vordergrund. In der Folge wird es nach Einführung des CMS

[194] Zu berücksichtigen ist bei der ISO 19600, dass es sich hier um einen Leitfaden handelt, der Empfehlungen beinhaltet.
[195] [195] IDW PS 980, Tz. 23, A20; ISO 19600, Zif. 9.2; ONR 192050, Zif. 8; TR CMS 101:2011, Zif. 8.
[196] siehe hierzu auch IDW PS 980, Tz 18.
[197] siehe hierzu Zif. 9.1.2.2.1 ISO/IEC 17021.

entsprechende Versuche geben, diese Kosten einzudämmen. Hier kann die Überprüfung ebenfalls helfen. Einerseits können durch Kosteneinsparungen entstehende Schwachstellen aufgedeckt werden, andererseits können prozessuale Synergien gefunden werden, die bei Aufrechterhaltung der notwendigen Sicherheit Prozesse und Kontrollen zusammenführen und damit eine optimale Kosteneffizienz herstellen.

Die relevanten Kriterien, der Umfang aber auch Häufigkeit und Methoden einer CMS Überprüfung sind vor dem Audit zu planen und in Ihrem jeweiligen Umfang einzugrenzen.

a) ***Interne Audits***

Interne Audits sind zunächst nicht an verbindliche Regeln gebunden. Es hilft hier aber – sofern es keine unternehmensinterne Richtlinie hierzu gibt – beispielsweise der „Leitfaden zur Auditierung von Managementsystemen“ nach ISO 19011, der für die Auditierung jeglicher Managementsysteme gilt.[198] Die Prüfung eines Managementsystems erfolgt danach in folgenden Stufen:

[198] In seinen Fassungen bis 2011 war die Norm auf die Auditierung von Qualitäts- und Umweltmanagementsystemen beschränkt, siehe DIN ISO 19011:2011, Nationales Vorwort, S. 2., Einleitung EN ISO 19011:2011, S. 4.

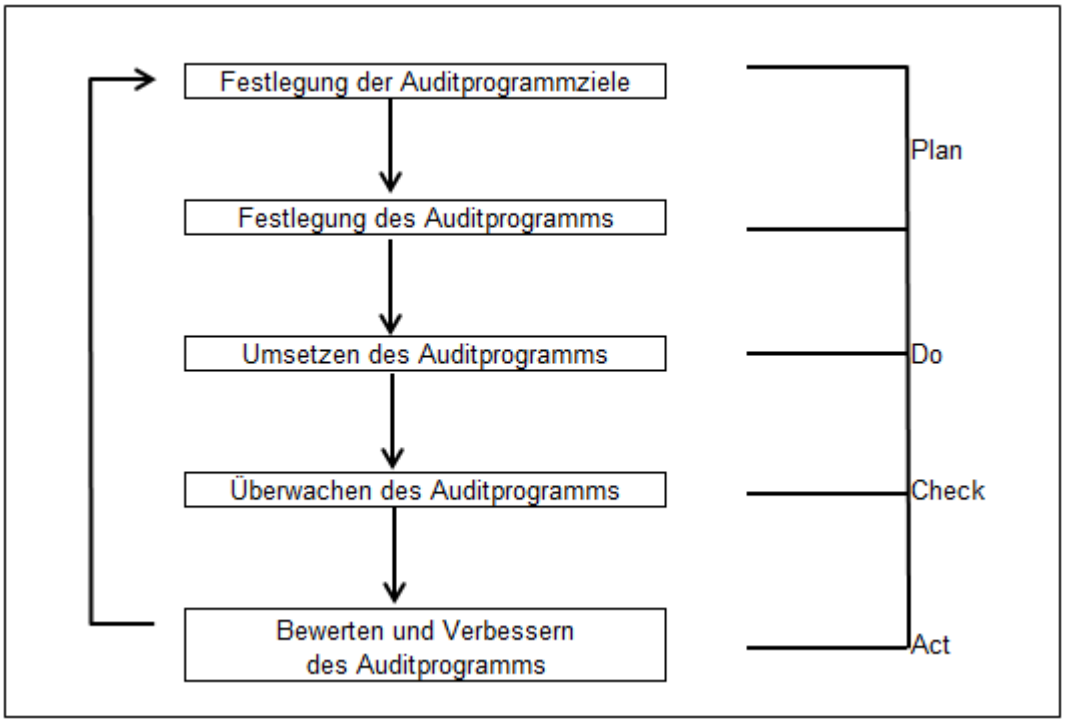

Abbildung 4: Prüfung eines Managementsystems nach ISO 19011[199]

b) ***Externe Audits und Zertifizierungen***

(1) Zertifizierung gem. ISO/IEC 17021

ISO/IEC 17021 legt die Anforderungen für eine Drittparteien-Zertifizierung von Managementsystemen fest.[200] Erfolgt eine solche Zertifizierung durch eine Zertifizierungsstelle auf Basis dieses Standards, bietet ein entsprechendes Zertifikat eine hohe Sicherheit für eine unabhängige, unparteiliche und neutrale Prüfung.[201]

Ein Auditprogramm nach ISO/IEC 17021 muss gem. Ziffer 9.1.1.2 der ISO/IEC 17021 ein zweistufiges Erstaudit, Überwachungsaudits im ersten und zweiten Jahr sowie ein Re-Zertifizierungsaudit im dritten Jahr unmittelbar vor Ablauf der Zertifizierung beinhalten. Ist die Erstzertifizierung auf Basis des zweistufigen

[199] Vereinfachte Darstellung auf Basis der Abbildung in DIN EN ISO 19011:2011, S. 15, Bild 1 - Auch hier wird der Deming Kreis als Basis für die Prüfung genutzt. Das Ziel der Prüfung ist damit klar auf die Erfassung des Ist-Zustands und die Verbesserung desselben ausgerichtet.
[200] In der ISO 19011:2011 wird aber darauf hingewiesen, dass die Nutzung der Anleitungen in dieser Norm auch bei der Drittparteien-Zertifizierung nützlich sein können - siehe Einleitung, DIN EN ISO 19011:2011, S. 4.
[201] Petsche-Toifl-Neiger-Jirges, S. 132.

Erstaudits erfolgreich, hat die Zertifizierung eine Gültigkeit von 3 Jahren. Eine Zertifizierung nach ISO/IEC 17021 liefert eine unabhängige Darlegung, dass das Managementsystem einer Organisation festgelegte Anforderungen erfüllt, in der Lage ist, ständig die festgelegte Politik und Ziele zu erreichen, und wirksam umgesetzt ist.[202]

Daneben gibt es Bestätigungen und sogenannte Zertifikate, beispielsweise durch Unternehmensberatungen oder Rechtsanwaltskanzleien, die bei der Einführung eines CMS unterstützen und beraten und dies bestätigen. Eine Einhaltung der durch ISO/IEC 17021 vorausgesetzten Grundsätze ist in diesen Fällen nicht gewährleistet.

Gerade das externe Compliance Audit – auch verbunden mit einer Zertifizierung – dient der Compliance Kultur im Unternehmen, da die Mitarbeiter weiter für das Thema sensibilisiert werden und ihr Compliance Bewusstsein gestärkt wird. Der Druck in der Vorbereitung des Audits, aber auch im Rahmen der Nacharbeiten führt dazu, dass Maßnahmen gesetzt werden, um das bestehende CMS systematisch zu strukturieren und zu dokumentieren, klare Organisationen zu schaffen und Verantwortlichkeiten festzulegen.[203] Die Prüfung durch Dritte verhindert Betriebsblindheiten und Interessenkonflikte.[204]

(2) Zertifizierung von ISO 19600

Ob ISO 19600 zertifizierbar sein wird, wird derzeit noch uneinheitlich beurteilt. Als Leitfaden wird ISO 19600 als sogenannte Typ-B Norm angesehen, die keine verbindlichen Requirements enthält.[205] Mangels verbindlicher Anforderungen wird der Standard daher teilweise als nicht zertifizierbar angesehen.[206] Daher überrascht es zunächst, wenn Austrian Standards ein sogenanntes „Fair Business® Compliance Certificate“ als Ergebnis der Prüfung

[202] DIN EN ISO/IEC 17021, Einleitung, S. 6.
[203] Berndt, BB 2012(14), VI-VII.
[204] Petsche-Toifl-Neiger-Jirges, S. 131.
[205] Makowicz, Compliance Praxis (Deutschland), 33ff. (33).
[206] Ehnert, Compliance Praxis (Deutschland), 58f. (59).

und Zertifizierung eines CMS nach ISO 19600 anbietet.[207] Begründet wird dies damit, dass die ISO 19600 als sog. Leitfaden einerseits Diskussionstext andererseits aber klare gekennzeichnete Empfehlungen enthalte. Die Implementierung einer solchen Empfehlung lasse sich jedoch nachprüfen und zertifizieren. In jedem Fall würden alle Empfehlungen der Norm umgesetzt werden müssen, um das Zertifikat zu erhalten. Mittels dieser Anforderung sei sichergestellt, dass aus den unverbindlichen Empfehlungen der Norm, verbindliche Kriterien zur Erlangung des Zertifikates würden. Auch würden die Zertifikate von Austrian Standards bestätigen, dass eine Organisation die Empfehlungen der ISO 19600 implementiert habe und deswegen ein CMS nach den Empfehlungen der ISO 19600 betreibe.[208]

Wie sich aus der Einleitung aber auch aus Zif. 4.1.2 der ISO/IEC 17021 ergibt, ist übergeordnetes Ziel von Zertifizierungen, allen Seiten das Vertrauen zu vermitteln, dass ein Managementsystem festgelegte Anforderungen erfüllt. Wenn ein Managementsystem nach dem Wunsch des jeweiligen Urhebers aber eben keine festgelegten Anforderungen (specified requirements) enthält, sondern lediglich ein Leitfaden ist, lässt sich vertreten, dass das Ziel der Zertifizierung nicht erfüllt werden kann.

Für eine umfassende Implementierung von Compliance und CMS im Wirtschaftsleben müssen auch kleinere und mittlere Unternehmen überzeugt werden, dass dies mit einem verhältnismäßigen Aufwand möglich ist. Weil es sich aber bei ISO 19600 ein aus Empfehlungen bestehendes Rahmenwerk handelt, hat dieser Standard einen großen Umfang und weißt eine erhebliche Detailtiefe auf. Die verbindliche Voraussetzung aller Empfehlungen als verbindliche Kriterien birgt daher die Gefahr einen hohen Aufwand bei der Implementierung zu fordern.

[207] siehe unter http://www.iso19600.org/fileadmin/user_FBCC/dokumente/zertifizierungsschema-compliance.pdf (05.12.2014).
[208] so P. Jonas, Director Certification, Austrian Standards plus GmbH in einer E-Mail an den Verfasser vom 03.12.2014.

Auch die anderen Standards sind aber – gerade aufgrund ihrer Kürze – interpretationsbedürftig und bieten damit eine geringere Klarheit. Die Grundsätze der Verhältnismäßigkeit und Flexibilität erlauben – mit der richtigen Begründung – notwendige Anpassungen auch bei ISO 19600.

ISO 19600 stellt unstreitig den neuesten Stand der Technik zum Thema CMS dar. Internationale Experten haben sich hier auf einen gemeinsamen Standard geeinigt, der auch und insbesondere im gerichtlichen Verfahren, von Sachverständigen berücksichtigt werden müsste. Unter Berücksichtigung dieses Umstands, erscheint die Frage, ob eine „Guideline“ nun durch das Wort „should“ gekennzeichnete Vorschläge enthält oder Anforderungen mittels „shall“ vorgeschrieben werden, als zweitrangig.

Enthält das „Fair Business® Compliance Certificate“ die Bestätigung, dass eine Organisation die Empfehlungen der ISO 19600 implementiert habe und deswegen ein CMS nach den Empfehlungen der ISO 19600 betreibt, so wird nicht der Eindruck erweckt, dass es sich bei ISO 19600 um verbindliche Anforderungen handelt.

(3) Testat nach IDW PS 980

Die Zertifizierung nach ISO/IEC 17021 ist nicht mit dem Testat des Wirtschaftsprüfers zu verwechseln, der eine Prüfung nach IDW PS 980 vornimmt.[209]

IDW PS 980 definiert in Tz. 12ff. Gegenstand, Ziel und Umfang der Prüfung. Das Ziel der Prüfung ist jeweils von der vereinbarten Prüfung und deren Umfang abhängig. Der Standard sieht diesbezüglich entweder eine Konzeptionsprüfung, eine Angemessenheitsprüfung oder eine Wirksamkeitsprüfung vor.[210] Abhängig vom jeweiligen Auftrag steigt der Prüfungsumfang.

[209] Berndt, BB 2012(14), VI-VII.
[210] IDW PS 980, Tz. 14ff.

Im Rahmen der Konzeptionsprüfung wird der Prüfer anhand der vom Unternehmen aufgestellten CMS-Grundsätze eine Aussage darüber treffen, ob „die in der CMS-Beschreibung enthaltenen Aussagen zur Konzeption des CMS in allen wesentlichen Bereichen angemessen dargestellt sind“. Dies ist dann der Fall, wenn sämtliche Grundelemente des CMS enthalten sind und wenn eine Irreführung der Berichtsadressaten aufgrund wesentlicher falscher Angaben, unangemessener Verallgemeinerungen oder unausgewogener und verzerrender Darstellungen möglich sind.

Die Angemessenheitsprüfung klärt zusätzlich ob die dargestellten Grundsätze und Maßnahmen in Übereinstimmung mit den CMS Grundsätzen geeignet sind, mit hinreichender Sicherheit sowohl Risiken für wesentliche Regelverstöße rechtzeitig zu erkennen und zu verhindern. Auch wird geprüft, ob die Grundsätze und Maßnahmen zu einem bestimmten Zeitpunkt implementiert waren.

Aufbauend auf den Beurteilungen zur angemessenen Darstellung der Aussagen zur Konzeption (Konzeptionsprüfung) und der Geeignetheit sowie Implementierung des CMS zielt die Wirksamkeitsprüfung darauf ab, eine Aussage zur Wirksamkeit des CMS in einem bestimmten Zeitraum zu treffen.

(4) Resümee

Unabhängig davon, ob nun eine interne oder externe Prüfung durch die interne Revision oder externe Prüfer, durch eine unabhängige Zertifizierungsstelle oder einen Wirtschaftsprüfer erfolgt – in jedem Fall dient die Prüfung jedenfalls der Verbesserung und Weiterentwicklung des jeweils geprüften CMS.

Ob eine vollständige Zertifizierung nach ISO/IEC 17021 oder ein Testat eines Wirtschaftsprüfers über die Implementierung eines wirksamen CMS nach IDW PS 980 angestrebt wird – beides wird im Rechtsverkehr aufgrund der hohen formalen Anforderungen sowohl an das jeweilige CMS aber auch an die zertifizierenden Stellen besonderes Vertrauen genießen dürfen. In allen Fällen

hat das zu zertifizierende Industrieunternehmen den Beweis zu erbringen, dass ein effektives CMS eingerichtet wurde, wodurch das Risiko von Compliance Verstößen soweit wie möglich gesenkt wird. Hervorzuheben bei ISO/IEC 17021 ist aber der vorgesehene 3 Jahres Zyklus der Zertifizierung samt der entsprechenden Überwachungsaudits und eines Re-Zertifizierungsaudits im 3 Jahr. Der IDW PS 980 sieht einen solchen Prozess nicht vor. Das Testat des Wirtschaftsprüfers enthält lediglich eine Aussage zum Status quo bzw. zur Vergangenheit. Die Entscheidung für eine Zertifizierung eines CMS nach ISO/IEC 17021 gibt diesen zukunftsgerichteten Prozess vor und wird zu einer nachhaltigen Implementierung eines wirksamen CMS führen können.

Auch wenn der Wirtschaftsprüfer seinen Berufsstandsregeln verpflichtet ist, wird dem entgegengehalten, dass die Zertifizierungsregeln der ISO/IEC 17021 die Unabhängigkeit, Unparteilichkeit und Neutralität der Zertifizierungsstelle garantiere. Demgegenüber sei davon auszugehen, dass beim IDW PS 980 oftmals die Einrichtung und Prüfung oder zumindest Beratung und „Zertifizierung“ [211] durch denselben Wirtschaftsprüfer erfolge. [212] Dieser Beratungsansatz wird in der dreistufigen Prüfung deutlich, die es dem Prüfer erlaubt, begleitend zur Einrichtung und Beratung den jeweiligen Stand des CMS zu testieren. Eine solche Konstellation erlaubt, die erforderliche Neutralität in Frage zu stellen.

3. Zusammenfassender Vergleich

Sowohl der TR CMS 101:2011 als auch ISO 19600 folgen dem PDCA-Zyklus. Auch wenn die beiden anderen CMS Standards sich nicht offensichtlich an Management-Systemen aus anderen Bereichen orientieren, bilden Sie gleichwohl einen vergleichbaren Zyklus ab, indem Sie ebenfalls einen kontinuierlichen Verbesserungsprozess voraussetzen.

[211] gemeint ist hier die Testierung.
[212] Petsche-Toifl-Neiger-Jirges, S. 132.

Aus der Darstellung der unterschiedlichen CMS Standards ist aber ersichtlich, dass bei aller Vergleichbarkeit Unterschiede im Detail zu finden sind.

In allen Standards wird die Verantwortung der Leitung bei der Implementierung von Compliance in der jeweiligen Organisation betont. Die Selbstverpflichtung der Leitung und deren Vorbildfunktion sind unverzichtbare Teile eines jeden CMS.[213] Lediglich die allein wortlautorientierte Auslegung von ONR 192050, Zif. 3 wird zu dem Ergebnis kommen, dass der Leitung der Organisation eher eine sicherstellende Wirkung denn eine aktives „Commitment" zu Compliance zukommt. Doch auch hier ist eine aktive Rolle der Leitung bei der Kommunikation des CMS und seiner Inhalte an die Organisationsmitglieder als notwendig anzusehen. Unterlagen und Dokumente sind hierfür durch die Leitung zugänglich zu machen. Aus der Kommentierung der ONR 192050 wird deutlich, dass auch hier ein proaktives und zielgerichtetes Verhalten der Organisationsleitung erwartet wird.[214]

Der IDW PS 980 verlangt die Festlegung von Compliance Zielen, also der in der jeweiligen Organisation einzuhaltenden Regeln.[215] Hierfür sind insbesondere die relevanten Teilbereiche festzulegen. Die in diesen Teilbereichen einzuhaltenden Regeln sind ebenfalls zu identifizieren. Abgrenzbare Teilbereiche können Geschäftsbereiche, Unternehmensprozesse, Rechtsgebiete oder auch regionale Einheiten sein.[216] Aber auch ISO 19600 und TR CMS 101:2011 sehen die Definition von einzuhaltenden Regeln vor.[217] ONR 192050 definiert den Begriff der „Regeln"[218]und nutzt diesen im Zusammenhang mit der erforderlichen Kenntnis des Compliance Officers über diese Regeln[219]

[213] siehe unter anderem ISO 19600, Zif. 5.1., 5.3.1, 5.3.2, 5.3.3; IDW PS 980, Tz 23, A15, A18; TR CMS 101:2011, Zif. 5; ONR 192950, Zif. 3.
[214] Petsche-Toifl-Neiger-Jirges, S. 34ff.
[215] IDW PS 980, Tz. 23.
[216] IDW PS 980, Tz. 6, A.3.
[217] ISO 19600, Zif. 4.5.1; TR CMS 101:2011, Zif. 7.2.
[218] Zif. 2.8: „jedenfalls alle Verpflichtungen, welche hoheitlich aufgestellt wurden und welche für die Organisation verbindlich sind. Die Organisation kann auch freiwillig eingegangene Verpflichtungen (zB vertragliche Verpflichtungen, interne Richtlinien) als relevante Regeln im Sinne dieser ONR festlegen."
[219] ONR 192050, Zif. 4.

sowie betreffend der Identifikation von Compliance-relevanten Vorgängen im Hinblick auf die Regeln[220].

Im IDW PS 980 fällt auf, wie sehr dieser Standard bei der Differenzierung dieser Ziele und Regeln auf abgrenzbare Teilbereiche abstellt. Dies geht soweit, dass ein CMS sich auf abgrenzbare Teilbereiche beziehen kann. Es können also in einer Organisation sogar verschiedene CMS in unterschiedlichen Teilbereichen bestehen.[221] Doch auch der ISO 19600 ist dieses Vorgehen nicht fremd. Vor einer Implementierung eines CMS sind auch hier die Grenzen und die Anwendbarkeit desselben zu definieren.[222]

Compliance Verantwortliche sind zu definieren (sei es als umfassend verantwortliche Mitarbeiter wie Compliance Officer oder in Form eines Compliance Gremiums). So sehen der IDW PS 980 in Tz. A18 und ISO 19600, Zif. 5.3.2, vor, einen Compliance Beauftragten oder ein Compliance Gremium zu benennen und entsprechenden Zuständigkeiten auszustatten. Nach ONR 192050 können eines oder mehrere Organisationsmitglieder die Aufgaben eines Compliance Officers wahrnehmen. TR CMS 101:2011 sieht hier lediglich die Auswahl und Benennung eines Compliance Beauftragten.[223]Lediglich die TR CMS 101:2011 schreibt verbindlich vor, dass dies ein Mitglied der Leitung zu sein hat. Diese Vorgabe birgt die Gefahr von Interessenkonflikten. Hier ist sorgfältig abzuwägen, ob und inwiefern die Leitungseigenschaft mit der Aufgabe des Compliance-Beauftragten vereinbar ist.

Die Identifizierung der Compliance Risiken bildet in allen Regelwerken die Basis für die Definition eines Compliance-Programms bzw. der notwendigen

[220] ONR 192050, Zif. 5.
[221] IDW PS 980, Tz. 6 - Dies ist zwar nicht undenkbar und ist der Effektivität – bezogen auf diese jeweiligen Teilbereiche – nicht unbedingt abträglich, jedoch stellt sich hier die Frage, ob dieses Vorgehen nicht im Hinblick auf die erforderlichen Ressourcen und Kosten optimierbar wäre.
[222] ISO 19600, Zif. 4.3.
[223] ONR 192050, Zif. 4, TR CMS 101:2011, Zif. 5.2.2.

Maßnahmen zur Reduktion der Compliance Risiken.[224] Hierfür müssen die notwendigen Ressourcen zur Verfügung gestellt werden.[225]

Nichtsdestotrotz gibt es Unterschiede, einerseits in der Gewichtung der Themen, andererseits bei Details, die teilweise konkret erwähnt werden, in anderen Standards bestenfalls hineinzuinterpretieren wären. So sieht der IDW PS 980 beispielsweise kein (anonymes) Hinweisgebersystem vor, sondern schreibt lediglich die Festlegung von Berichtswegen vor,[226] während in den anderen hier untersuchten Standards ein Hinweisgebersystem vorausgesetzt wird[227].

Der IDW PS 980 wiederum betont die Schaffung einer Compliance Kultur. Der Begriff der Compliance Kultur wird weder in der ONR 192050 noch im TR CMS 101:2011 genannt, wohl aber in ISO 19600[228]. Unzweifelhaft ist dies aber die gewollte Folge des Tone from the Top[229] und somit nach jedem Standard von Bedeutung.

Kommunikation[230] und Training[231] sind als unabdingbare Elemente in allen Standards erwähnt, so wie im Übrigen auch alle die Überwachung des CMS als Basisbedingung für die Überprüfung der Wirksamkeit und Identifikation eventueller Schwachstellen vorsehen.[232] Auch wird immer die Verbesserung des CMS als Ziel genannt.[233] Die Definition von Compliance Kennzahlen zur

[224] ONR 192050, Zif. 5, IDW PS 980, Tz. 23, A16; ISO 19600, Zif. 4.6; TR CMS 101:2011, Zif. 7.1.
[225] ONR 192050, Zif. 3, IDW PS 980, Tz. 23, A18; ISO 19600, Zif. 7.1; TR CMS 101:2011, Zif. 6.1.
[226] IDW PS 980, Tz. A19.
[227] ISO 19600, Zif. 9.1.3 (Empfehlung); ; TR CMS 101:2011, Zif. 7.7; ONR 192050, Zif. 8.
[228] ISO 19600, Zif. 7.3.2.3.
[229] Petsche-Toifl-Neiger-Jirges, S. 33ff; Moosmayer, S. 47.
[230] ONR 192050, Zif. 9, IDW PS 980, Tz. 23, A19; ISO 19600, Zif. 7.4; TR CMS 101:2011, Zif. 5.2.3.
[231] ONR 192050, Zif. 7; IDW PS 980, Tz. 23, A19f.; ISO 19600, Zif. 7.2; TR CMS 101:2011, Zif. 6.2.2.
[232] ONR 192050, Zif. 8; IDW PS 980, Tz. 23, A20.; ISO 19600, Zif. 9; TR CMS 101:2011, Zif. 8.
[233] ONR 192050, Zif. 8; IDW PS 980, Tz. 23, A20.; ISO 19600, Zif. 10; TR CMS 101:2011, Zif. 8.3.

Messung der Wirksamkeit des CMS ist ausdrücklich in ISO 19600 und TR CMS 101:2011 vorgesehen.[234]

ISO 19600 betont auch die Bedeutung der externen Kommunikation[235] (auch wenn die Kommunikation von Informationen ggf. auch an Dritte im IDW PS 980 kurz erwähnt wird[236]).

Der TR CMS 101:2011 enthält die Voraussetzung eines Systems von Freigaben, Genehmigungen und Berechtigungen.[237] Ebenfalls fällt im TR CMS 101:2011 durch die Aufzählung üblicher Vorgabedokumente und Verfahren zur Lenkung von Vorgabe- und Nachweisdokumenten auf, wie dokumentationszentriert dieser ist.[238] Der TR CMS 100/2013 unterstützt diesen Eindruck durch die Aufzählung von Dokumentationsbeispielen als Nachweis für die Einhaltung der Anforderungen des Standards. Es ist aber zu berücksichtigen, dass die umfassende Dokumentation des CMS und aller Compliance-relevanten Aktivitäten unabhängig von der Art des gewählten Standards erforderlich ist. Nur hierdurch ist es möglich, die Einhaltung der jeweiligen Voraussetzungen zu überprüfen und gegebenenfalls auch zu zertifizieren.

III. ERGEBNISSE UND AUSBLICK

Mit Ausnahme des Bank- und Kapitalmarktrechts ist Compliance und insbesondere Compliance in der produzierenden Industrie derzeit kein Thema der Europäischen Union. Mit der 8. EU- Richtlinie („Abschlussprüfer-Richtlinie")[239] und der Änderungsrichtlinie[240] wurde in Folge von SOA ein eher dünnes Fundament für die Harmonisierung der europäischen Rechtssysteme

[234] ISO 19600, Zif. 9.1; ; TR CMS 101:2011, Zif. 8.2, 8.3.1.
[235] ISO 19600, Zif. 7.4.
[236] IDW PS 980, Tz. 23.
[237] TR CMS 101:2011, Zif. 7.6.
[238] TR CMS 101:2011, Zif. 4.2.
[239] s.o. S. 35 ff.
[240] s.o. S. 37 ff.

gelegt. Diese beschränken sich auf die Begrenzung finanzieller und betrieblicher Risiken sowie des Risikos von Vorschriftenverstößen auf ein Mindestmaß. Insbesondere kann hier die verpflichtende Einrichtung von Prüfungsausschüssen und wirksamen internen Kontrollsystemen in „Unternehmen von öffentlichem Interesse“ [241] und die Verpflichtung börsennotierter Unternehmen, dieses IKS im Lagebericht zu erläutern, genannt werden.

Auch wenn es eines der erklärten Ziele der Europäischen Kommission ist, den Rechtsrahmen für „Corporate Governance“ zu reformieren und Compliance Teil derselben ist, haben die europäischen Organe in den untersuchten Quellen bisher zu diesem Thema geschwiegen.[242] Ob sich daran in Hinkunft etwas ändert, wird sich weisen.

Es kann davon ausgegangen werden, dass bei „Unternehmen von öffentlichem Interesse“ im Sinne des iSd Art. 2 Nr. 13 Abschlussprüfer-Richtlinie (Aktiengesellschaften und Societas Europaea, deren Aktien an Börsen gehandelt werden, Kreditunternehmen und Versicherungsunternehmen) Systeme, die Compliance im Unternehmen zum Ziel haben, verpflichtender Teil des IKS sind.[243]

Aufgrund der genannten Regelungen des nationalen Rechts[244] besteht aus der Leitungsverantwortung die Verpflichtung, im jeweils erforderlichen und angemessenen Umfang ein CMS einzuführen, [245] wenn die individuellen Compliance Risiken einen Komplexitätsgrad erreichen, der die Gefahr begründet, dass rechtliche Vorgaben nicht eingehalten werden, also eine „abstrakte Gefährdungslage“ besteht (sog. Legalitätskontrollpflicht). [246]

---

[241] s.o. S. 36.
[242] s.o. S. 46f.
[243] s.o. S. 47f.
[244] s.o. S. 39ff.
[245] s.o. S. 48.
[246] Markfort, ZRFC 2014, 180 (181) in der Besprechung von LG München I v. 10.12.2013 - 5HK O 1387/10, AG 2014, 332-336.

Daher werden alle Unternehmen, also auch die kleineren und mittleren Industrieunternehmen, sich kritisch damit auseinander setzen müssen, ob es sinnvoll und notwendig sein wird, ein CMS einzuführen und dieses regelmäßig prüfen und vielleicht sogar zertifizieren oder testieren zu lassen.

Hierbei ist zu berücksichtigen, dass es keine preisgünstige „one fits all"-Lösung gibt. So einzigartig wie die Industrieunternehmen, ihre Organisation und ihr jeweiliges Geschäft sind, so individuell ist das notwendige CMS. Abhängig vom jeweiligen Compliance Risiko sind genau die Maßnahmen zu definieren, die dieses Risiko im erforderlichen Umfang adressieren.

Im Sinne des klassischen Kreislaufs im Risikomanagement ist hierfür zunächst in allen Fällen mit Hilfe einer Risikoidentifikation festzustellen, welche individuellen Compliance Risiken bestehen. Diese Risiken sind unter Berücksichtigung der Wahrscheinlichkeit und Auswirkung zu bewerten. Anschließend sind bei den identifizierten und nicht unwahrscheinlichen Risiken Maßnahmen zu definieren, wie diese Risiken ausgeschlossen bzw. auf das notwendige Mindestmaß reduziert werden können.[247]

Unabhängig von der Größe des jeweiligen Industrieunternehmens muss daher gelten, dass der Reifegrad und damit auch die Anforderungen an das jeweilige CMS vom Umfang der Risiko-Exposition abhängt.

[247] Daran schließt sich ein entsprechendes Controlling und Reporting an, dem wiederum die erneute Risikoidentifizierung folgt, um festzustellen, ob und wie die jeweiligen Maßnahmen gegriffen haben – siehe auch Denk/Exner-Merkelt/Ruthner, S. 82.

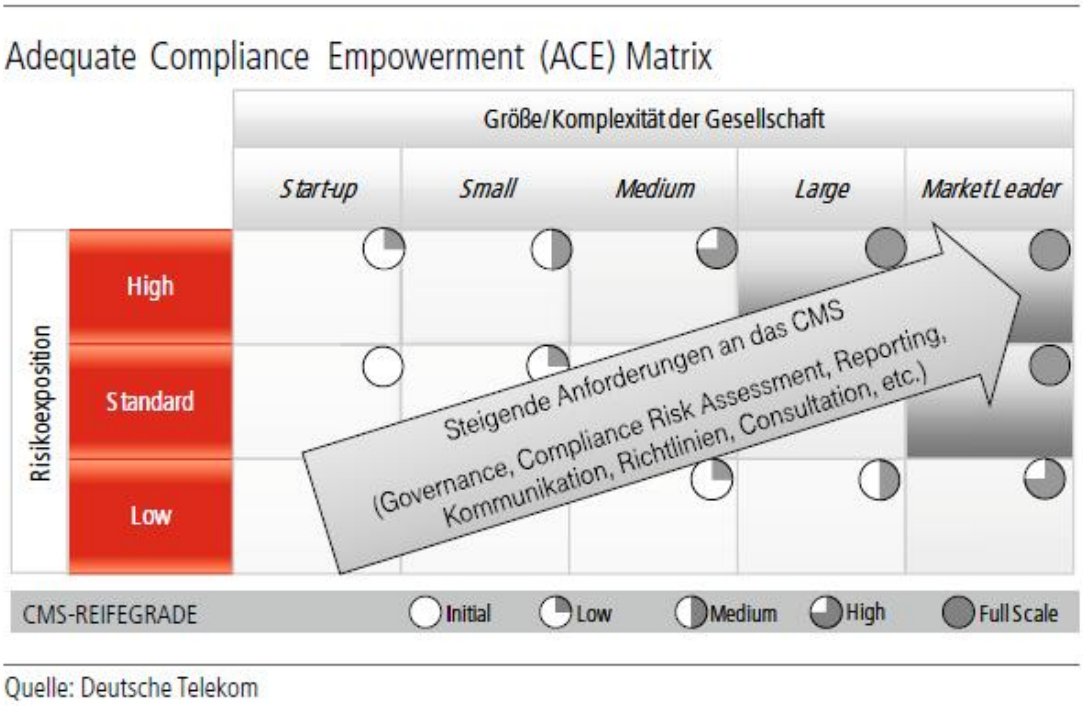

Abbildung 5: Anforderungen an den Reifegrad eines CMS[248]

Compliance Management Systeme können hierbei oftmals auf bestehenden Systemen wie IKS, Risikomanagement und/oder interner Revision und Rechtsabteilung aufbauen bzw. vorhandene Ressourcen nutzen.

Bei der Implementierung eines CMS helfen die bestehenden CMS Standards. Industrieunternehmen im deutschsprachigen Raum haben die Wahl zwischen den deutschsprachigen Standards IDW PS 980, dem TR CMS 101:2013 und dem ONR 192050. Hinzu kommt der Standard ISO 19600, der bisher nur in englischer Sprache verfügbar ist. Es ist sinnvoll, das in diesen Standards vorhandene Know-How zu nutzen und sich bei Planung und Aufbau des CMS entsprechend leiten zu lassen.

Ob eine vollständige Zertifizierung nach ISO/IEC 17021 oder ein Testat eines Wirtschaftsprüfers über die Implementierung eines wirksamen CMS nach IDW

[248] Abbildung aus „Compliance“, Juni 2014, S. 8 - http://compliance-plattform.de/uploads/media/Compliance-06-2014.pdf?utm_source=CleverReach&utm_medium=email&utm_campaign=13-06-2014+Compliance+Juni+2014&utm_content=Mailing_7723337 (13.06.2014).

PS 980 angestrebt wird – beides wird im Rechtsverkehr aufgrund der hohen formalen Anforderungen sowohl an das jeweilige CMS aber auch an die zertifizierenden Stellen besonderes Vertrauen genießen dürfen. In allen Fällen hat das zertifizierte Industrieunternehmen den dokumentierten Beweis zu erbringen, dass ein effektives CMS eingerichtet wurde, wodurch das Risiko von Compliance Verstößen soweit wie möglich gesenkt wird. Zu berücksichtigen ist aber, dass IDW PS 980 nur den Status quo prüft. Die Zertifizierung eines CMS nach ISO/IEC 17021 erfolgt im 3-Jahres Rhythmus und ist – auch aufgrund der regelmäßigen Überwachungsaudits –immer auf dem neuesten Stand.

Offensichtlich ist der hohe Detaillierungsgrad des ISO 19600 im Vergleich zu den dargestellten deutschsprachigen Standards. Als wesentlicher Grund hierfür erscheint der Umstand, dass es sich bei ISO 19600 um einen Leitfaden handelt, der Empfehlungen und Lösungsansätze für ein effektives CMS darstellt. Relativiert wird diese Detailtiefe insbesondere durch die Grundsätze der Flexibilität und Verhältnismäßigkeit,[249] die dazu beitragen, dass das CMS an Größe, Bedarf und Risikolage der Organisation angepasst werden kann.[250] Die Entwicklung und Implementierung bzw. operative Umsetzung eines CMS ist demnach bei Nutzung des ISO 19600 als Richtschnur und als Anleitung möglich. Ein CMS nach ISO 19600 kann aufgrund der High Level Structure in bestehende Management Systeme im Unternehmen integriert werden. Dies ist eine wesentliche Basis für die Anerkennung und Nutzung der ISO 19600 als weltweiter Standard.

Auch IDW PS 980, TR CMS 101:2013 und ONR 192050 werden aber weiterhin als Basis für ein CMS dienen können. Die österreichische Lösung der Zertifizierung nach ISO 19600 wird im Wettbewerb zu den nationalen CMS Standards zumindest das Argument zu entkräften haben, dass die verbindliche

[249] ISO 19600, Zif. 1.
[250] so auch Bartosz Makowicz in einem Interview mit Reinhard Preusche (Vorsitzender des Vorstandes des Netzwerk Compliance e.V., Frankfurt) im November 2014, siehe unter http://www.netzwerk-compliance.de/fileadmin/content/PDF/Veroeffentlichungen/Interview_DIN_ISO19600_14nov19.pdf.

Voraussetzung aller Empfehlungen als verbindliche Kriterien einen hohen Aufwand bei der Implementierung fordert. Dies sollte aber auch mit dem Hinweis auf den Grundsatz der Verhältnismäßigkeit und Flexibilität gelingen.

Sofern die kürzeren „nationalen“ Standards aber weiter entwickelt werden, können sie auch in Zukunft ihre Berechtigung behalten. Insbesondere besteht in ihnen die Chance – die bisher noch nicht offensichtlich wahrgenommen wurde – die Anforderungen der nationalen Rechtssysteme und –kulturen zu berücksichtigen, die durch die jeweils geltenden Gesetze und Präjudizien geprägt werden. Ob dies in einem internationalen Standard immer möglich sein wird, erscheint fraglich. CMS werden auch zukünftig an nationalen Anforderungen gemessen werden. Wenn es gelingt, sowohl den in der ISO 19600 dargestellten internationalen Stand der Technik als auch die nationalen Anforderungen in den anstehenden Revisionen der CMS Standards IDW PS 980, TR CMS 101:2013 und ONR 192050 zu berücksichtigen, werden diese auch weiterhin eine Zukunft haben.

LITERATURVERZEICHNIS

Bernd, Thomas	Zertifizierung von Compliance-Management-Systemen als neues Geschäftsfeld, in Betriebs-Berater, 2012(14), S. VI-VII.
Borchardt, Klaus-Dieter	Die rechtlichen Grundlagen der Europäischen Union, 4. Auflage, Wien 2010 (zit.: Borchardt, §, Rz.).
Busch, Jörg / Hjertonsson, Sonja	Sieben Elemente eines effizienten und wirksamen Compliance-Management-Systems, in CFOaktuell 2013, S. 96ff.
Denk, Robert; Exner-Merkelt, Karin; Ruthner, Raoul	Corporate Risk Management, 2. Auflage, Wien 2008 (zit.: Denk/Exner-Merkelt/Ruthner, S.).
Donner, Gerhard	Corporate Compliance - Risiken, Herausforderungen, Maßnahmen und Nutzen, in CFOaktuell 2012, S. 20ff.
Dreher, Meinrad	Die Vorstandsverantwortung im Geflecht von Risikomanagement, Compliance und interner Revision, in Festschrift für Uwe Hüffer, München 2010.
Ehnert, Manja	Wie hilfreich sind ISO-Normen für Compliance, in Compliance Praxis (Deutschland), Service Guide 2014, S. 58f.

Feltl, Christian / Pucher, Michael	Corporate Compliance im österreichischen Recht - Ein Überblick, wbl 2010, S. 265ff.
Görtz, Birthe	Prüfung von Compliance-Management-Systemen, Anwendung und Erfahrungen mit IDW PS 980, in Betriebs-Berater 2012, S. 178ff.
Goette, Wulf / Habersack, Matthias / Kalss, Susanne	Münchner Kommentar zum Aktiengesetz Band 2, §§ 76-117, 3. Auflage, München 2008 (zit.: MüKo-Bearbeiter, §, Rz.).
Habersack, Mathias / Drinhausen, Florian	SE-Recht mit grenzüberschreitender Verschmelzung, München 2013 (zit.: Habersack/Drinhausen/Bearbeiter, §, Rz.).
Habersack, Mathias	Europäisches Gesellschaftsrecht, München 2006 (zit.: Habersack, §, Rz.)
Hagel, Ulrich / Dahlendorf, Jana	Der Beitrag von Wirtschaftsverbänden zur Compliance am Beispiel des „Rundum-Paketes“ des Verbandes der Bahnindustrie in Deutschland (VDB), in CCZ 2014, S. 275ff.
Hauschka, Christoph E.	Corporate Compliance, 2. Aufl., München 2010 (zit. Hauschka/Bearb., Abschnitt, §, Rz.).

Hausmaninger, Christian / Kletter, Mark / Burger, Ernst:	Der österreichische Corporate Governance Kodex, Kurzkommentar, 1. Auflage, Wien 2003 (zit.: Hausmaninger/Kletter/Burger, Kap., Rz.).
Hausmaninger, Christian / Gratzl, Martin / Justich, Georg	Handbuch zur Aktiengesellschaft, Wien 2013 (zit. Bearb. in Hausmaninger/Gratzl/Justich, Kap., Rz.).
Hüffer, Uwe	Aktiengesetz, 10. Auflage, München 2012 (zit.: Hüffer, §, Rz.).
Kindl, Caroline / Petsche, Alexander	Compliance im Steuerrecht, Compliance-Praxis 1/2013, S. 14ff.
Kreuzer, Christian	Compliance, in CFOaktuell 2009, S. 205.
Makowicz, Bartosz	Wie ISO-bereit ist Ihr CMS?, in Compliance Praxis (Deutschland), Service Guide 2014, S. 33ff.
Markfort, Rainer	Verantwortung der Geschäftsleitung für Compliance, ZRFC 2014, S. 180 ff.
Messow, Bastian Rolf Winfried	Die Anwendbarkeit des Deutschen Corporate Governance Kodex auf die Societas Europaea (SE), Frankfurt a.M. 2008, zugl. Würzburg, Univ. Diss, 2007 (zit.: Messow, S.).

Moosmayer, Klaus	Compliance Praxisleitfaden für Unternehmen, 2. Auflage München 2012 (zit. Moosmayer, S.)
Napokoj, Elke	Risikominimierung durch Corporate Compliance; Wien 2010, (zit. Napokoj, Rz.).
Petsche, Alexander / Mair, Karin	Handbuch Compliance, 2. Auflage, Wien 2012, (zit. Bearb. in Petsche/Mair, S.).
Petsche, Alexander / Toifl Armin Neiger Barbara /Jirges, Elfriede	Compliance Management Systeme (CMS) - Die ONR 192050, 1. Auflage, Wien 2013 (zit. Petsche-Toifl-Neiger-Jirges, S.).
Petsche, Alexander / Trafoier, Christoph	Die Zertifizierung von CMS nach einem Wirtschaftsstandard wird Wirklichkeit, in Compliance Praxis 2013, S. 6 (Heft 1).
Petsche, Alexander / Dechant Georg	ISO 19600: Ein Weltstandard für Compliance-Management-Systeme entsteht, in Compliance Praxis 2014, S. 14 (Heft 3).
Rotsch, Thomas	Criminal Compliance, in ZIS 2010, S. 614 ff.
Sartor, Franz J./ Bourauel, Corinna	Risikomanagement kompakt: In 7 Schritten zum aggregierten Nettorisiko des Unternehmens, München 2013 (zit. Sartor/Bourauel, S.).

Schiel, Andreas — Beurteilung des Risikos wesentlicher Falschangaben im Jahresabschluss aufgrund von Bilanzmanipulationen – eine empirische Analyse, Dissertation, Technische Universität Dortmund, Februar 2011 (zit.: Schiel, S.).

Schneider, Uwe H. — Compliance als Aufgabe der Unternehmensleitung, in ZIP 2003, S. 645ff.

Starke, Philipp — Section 404 des Sarbanes-Oxley Act – Eine Untersuchung ihrer Auswirkungen auf Rechnungslegung, Abschlussprüfung und den Kapitalmarkt, Dissertation der Universität St. Gallen, St. Gallen 2006 (zit.: Starke, S.).

Strauch, Mark — Der Sarbanes-Oxley Act und die Entwicklungen im US-Aufsichtsrecht, in NZG 2003, S. 952.

Sturm, Maria Elisabeth — Corporate Governance – Die Umsetzung der Kommissionsempfehlungen in Deutschland und Österreich, Masterthesis, Universität Wien 2009, (zit. Sturm, Kap., S.).

Reitenbach, Enrico — „Die Beendigung der GmbH – systematische Darstellung und Möglichkeiten“, Dissertation, Universität Wien 2010 (zit. Reitenbach, S.)

Römermann, Volker — 2014 - ein Jahr im Zeichen der Compliance: nun auch für mittelständische GmbH, in GmbHR 2014, S. 1ff

Zöllner, Wolfgang/Noack, Ulrich — Kölner Kommentar zum Aktiengesetz, Bd. 2/1, §§ 76-94 AktG, 3. Auflage, Köln 2010 (zit.: Kölner Kommentar – Bearbeiter, §, Rz.).

DOKUMENTE / NORMEN / STANDARDS

Dokumente

Compliance matters	What companies can do better to respect EU competition rules; European Commission, European Union 2012
Europäische Kommission (KOM(2011) 164/3)	GRÜNBUCH Europäische Kommission - Corporate Governance-Rahmen vom 5.4.2011 (final)
Europäische Kommission (KOM(2011) 293 endgültig)	Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Schutz der finanziellen Interessen der Europäischen Union durch strafrechtliche Vorschriften und verwaltungsrechtliche Untersuchungen Gesamtkonzept zum Schutz von Steuergeldern
Europäische Kommission (KOM(2011) 573 endgültig)	Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Auf dem Weg zu einer europäischen Strafrechtspolitik: Gewährleistung der wirksamen Durchführung der EU-Politik durch das Strafrecht

Europäische Kommission (KOM(2012) 740 final)	Aktionsplan Europäisches Gesellschaftsrecht und Corporate Governance - ein moderner Rechtsrahmen für engagiertere Aktionäre und besser überlebensfähige Unternehmen, v. 12.12.2012
Europäisches Parlament (P7_TA(2012)0118)	Entschließung des Europäischen Parlaments v. 29. März 2012 zu einem Corporate Governance-Rahmen für europäische Unternehmen (2011/2181(INI))
Europäischer Wirtschafts- und Sozialausschuss (INT/678)	Stellungnahme zu […] Aktionsplan Europäisches Gesellschaftsrecht und Corporate Governance – ein moderner Rechtsrahmen für engagiertere Aktionäre und besser überlebensfähige Unternehmen COM(2012) 740 final v. 22. Mai 2013
ESMA Leitlinien	Leitlinien zu einigen Aspekten der MiFID-Anforderungen an die Compliance-Funktion; Dokument ESMA / 2012 / 388 der Europäischen Wertpapier- und Marktaufsichtsbehörde v. 25. Juni 2012
ISO/IEC Directives, Part 1	Consolidated ISO Supplement —Procedures specific to ISO, Fifth edition, Genf 2014

Standards und Normen

IDW PS 980	IDW Grundsätze ordnungsgemäßer Prüfung von Compliance Management Systemen – Stand: 11.03.2011; IDW Verlag GmbH, Düsseldorf 2011
DIN EN ISO/IEC 17021	Konformitätsbewertung – Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren (ISO/IEC 17021:2011), DIN Deutsches Institut für Normung e. V., Berlin
ISO 19600:2014 (E)	Compliance management systems – Guidelines, ISO copyright office, Genf 2014
ONR 192050:2013	Compliance Management Systeme (CMS) – Anforderungen und Anleitungen zur Anwendung; Austrian Standards Institute – Österreichisches Normungsinstitut, Wien 2013
TR CMS 101:2011	Standard für Compliance Management Systeme (CMS) des TÜV Rheinland: Köln 2011
TR CMS 100:2013	Compliance Leitfaden, TÜV Rheinland Cert GmbH, Köln 2013