Schwarzbartl/Pyrcek

Fachbuch Wirtschaft

Compliance Management

Ein Leitfaden zur erfolgreichen Umsetzung

Linde international

1. Corporate Compliance – Grundlagen

1.1. Definition und Grundlagen

Corporate (oder auch Criminal) Compliance ist in den letzten Jahren – insb. auf Basis von zahlreichen Unternehmensskandalen – vermehrt in den organisatorischen Fokus internationaler und nationaler Unternehmen gerückt. Rechtskonformes Verhalten, Sicherstellung von Integrität und die Vermittlung von Sicherheit lassen sich in heutiger Form nicht mehr von selbst darstellen und sicherstellen. Ebenso fördern Entwicklungen der nationalen und internationalen Gesetzgebungen, Standards und Normen die Komplexität der Systeme und – im Falle von strukturiertem Fehlverhalten – die mögliche Haftung von Unternehmensorganen. Demzufolge werden unternehmenseigene Management-Systeme zur Steuerung und Sicherstellung von rechtskonformen Verhalten, Ethik und Werten geschaffen – kurz: Compliance-Management-Systeme.

Hierbei sind die Definitionen des Begriffs Corporate oder Criminal Compliance in der Literatur sehr vielfältig. Doch im Kern ist diese Definition auf folgenden Mindestinhalt zu minimieren:

> *Unter Compliance ist die Einhaltung von Regeln zu verstehen (gesetzliche Bestimmungen und unternehmensinterne Richtlinien).*[1]

Der Begriff Compliance hat hierbei schon eine lange Vergangenheit – auch wenn dies nicht immer mit betriebswirtschaftlich-juristischem Kontext in Verbindung zu bringen ist. Die erstmalige hauptsächliche Verwendung des Begriffs ist vielmehr aus der Medizin und Pharmazie ableitbar, aus der sich das therapiekonforme Verhalten eines Patienten ableiten lässt. Die sog. Verordnungstreue beschreibt hierbei die korrekte Befolgung von Ratschlägen, Untersuchungen und Behandlungen. Aus dieser Definition lassen sich auch die drei Grundpfeiler eines Compliance-Management-Systems (CMS) wie folgt ableiten:

- **Prävention** = Vermeidung von möglichen Krankheiten
  (durch vorbeugende Einnahme von pharmazeutischen Produkten zur Vermeidung von Krankheiten gemäß ärztl. Verordnung, Lebensstil etc.)
- **Detektion** = Identifikation von möglichen Krankheiten und deren Symptomen
  (anhand von Untersuchungen etc.)
- **Reaktion** = Aufklärung und Behandlung von möglichen Krankheiten
  (durch ärztliche Behandlung etc.)

Doch nicht nur in der Medizin wurde auf den Begriff Compliance verwiesen, sondern u.a. auch in der US-Exportkontrolle während des Kalten Kriegs, dem angloamerikanischen Bankenwesen sowie der Prävention in Kartellverstößen wurde frühzeitig der Begriff der Compliance sinngemäß verwendet.[2]

---

1 *Institut der Wirtschaftsprüfer*, IDW PS 980, Tz. 5.
2 Vgl. *Eufinger, Alexander* (2012), S. 21 f.

Dabei sind Compliance und Compliance-Management per se keine neu geschaffenen Funktionen in einem Unternehmen. Auch vor der Schaffung sogenannter Integritäts-, Compliance- oder Ethik-Verantwortlicher wurden Funktionen, Prozesse und Kontrollen etabliert, welche die Sicherstellung rechtskonformen Verhaltens sicherstellen sollten. Erst aufgrund der großen Unternehmensskandale der jüngsten Vergangenheit wurden strukturelle Organisationen und Systeme etabliert, die ein gesamthaftes Integritäts- und Wertemanagement in einem Unternehmen sicherstellen sollen.

Aus dieser Perspektive wäre es somit falsch, zu folgern, dass Compliance-Funktionen etwas gänzlich Neues in einem Unternehmen darstellen – vielmehr ist Compliance und Compliance-Management nur der Prozess, der es erlaubt, diese spezifischen Risiken strukturiert im Rahmen eines Compliance-Management-Systems zu identifizieren, darauf zu reagieren, diese zu mitigieren und in weiterer Folge zu steuern und überwachen.

1.2. CMS-Rahmenkonzepte

Um ethisches Handeln im Unternehmen zu manifestieren, werden unternehmensspezifische Systeme, Prozesse und Kontrollen etabliert, welche präventiv, detektiv sowie reaktiv wirken sollen. Zur Ausgestaltung dieser Systeme existiert bereits eine Vielzahl an nationalen und internationalen Standards – auf wesentliche wird in diesem Kapitel eingegangen.

Unter einem Compliance-Management-System (CMS) sind die auf der Grundlage von festgelegten Zielen eingeführten Grundsätze sowie organisatorische und prozessuale Maßnahmen eines Unternehmens zu verstehen, die auf die Sicherstellung eines regelkonformen Verhaltens der gesetzlichen Vertreter und der Mitarbeiter des Unternehmens sowie ggf. von Dritten abzielen. Ziel ist die Einhaltung bestimmter Regeln und damit auch die Verhinderung von wesentlichen Rechtsverstößen. Das CMS zielt hierbei auf wesentliche Compliance-Risiken des Unternehmens ab.[3]

Das sog. Drei-Säulen-Modell der Compliance (oder auch Compliance-Haus) stellt ein Management-System dar, welches sich bei einer Vielzahl von nationalen und internationalen Unternehmen als gängiges Rahmenwerk zur Umsetzung von Compliance in einem Unternehmen durchgesetzt hat. Dieses orientiert sich an den Elementen der medizinisch-pharmazeutischen Definition:

[3] Vgl. *Institut der Wirtschaftsprüfer*, IDW PS 980, Tz. 6.

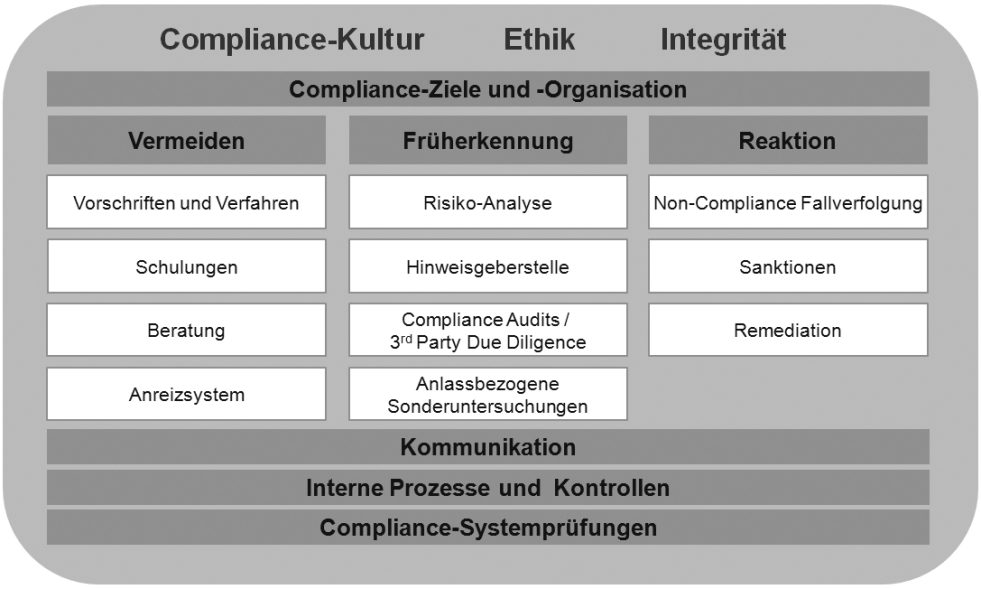

Abb. 1: Compliance-Haus

An dieser Stelle soll festgehalten werden, dass ein CMS ein System ist, welches zwar auf Best-Practice von nationalen und internationalen Unternehmen basieren kann, jedoch immer auf die eigene bestehende Unternehmenskultur und -organisation, Risikosituation etc. angepasst werden muss. Aus diesem Grunde können national und international entwickelte Rahmenkonzepte für Compliance und Ethik lediglich einen Orientierungsrahmen zur Ausgestaltung eines Compliance-Management-Systems bieten.

Einzelne internationale Standards nehmen in der Compliance-Branche jedoch gesonderten Status ein:

- **US Federal Sentencing Guidelines Manual – Chapter 8b –** Remedying harm from criminal conduct, and effective compliance and ethics program:[4]
  Das US Federal Sentencing Guidelines Manual (USSG) ist ein Grundelement zur Sanktionierung von unternehmerischem Fehlverhalten nach dem US Foreign Corrupt Practices Act (FCPA) – einer der global strengsten Anti-Korruptions-Gesetzgebungen mit munltinationaler Relevanz. Der FCPA verbietet im Wesentlichen das Anbieten, Versprechen, Leisten, Genehmigen und/oder Gewähren von Vorteilen jeglicher Art („anything of value") an einen ausländischen Amtsträger in der unredlichen Absicht, diesen zu beeinflussen, um geschäftliche oder sonstige unlautere Vorteile zu erlangen oder zu sichern. Zudem werden Falschaussagen in der Finanzberichterstattung oder im Jahresabschluss unter Strafe gestellt („accurate books and records"). Die Relevanz des Gesetzes erstreckt sich hier jedoch nicht ausschließlich auf US-Unternehmen.

4 *United States Sentencing Commission* (2011), o.S.

Nach dieser Jurisdiktion wurden jüngst Unternehmen wie Siemens, Deutsche Telekom, Johnson & Johnson, KBR/Halliburton oder auch Panalpina zu hohen Strafzahlungen verurteilt.[5]

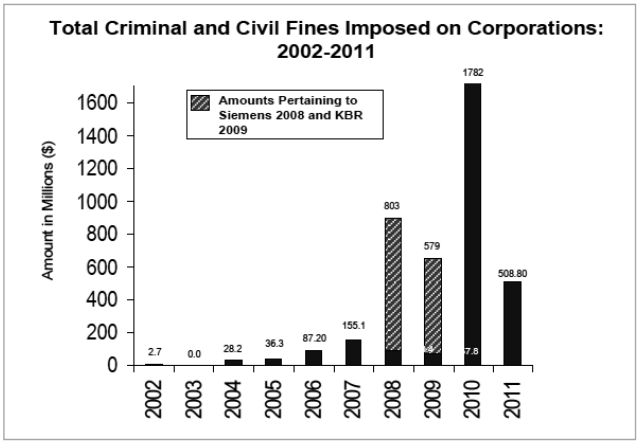

Abb. 2: Historie von Strafzahlungen nach dem FCPA[6]

Das US Federal Sentencing Guidelines Manual – insb. Chapter 8b („Remedying harm from criminal conduct, and effective compliance and ethics program") – nimmt eine gesonderte Rolle ein. Dieses Kapitel der US-amerikanischen Gesetzgebung beschreibt die Grundelemente einer effektiven Compliance- und Ethik-Organisation eines Unternehmens. Im Rahmen der Strafbemessung und Sanktionierung nach einem FCPA-Verstoß wird ein sog. Culpability-Score ermittelt, über den das Ausmaß der Strafzahlung beziffert wird. Ein ausreichend gestaltetes Compliance System nach den USSG wirkt sich hierbei strafmildernd aus.

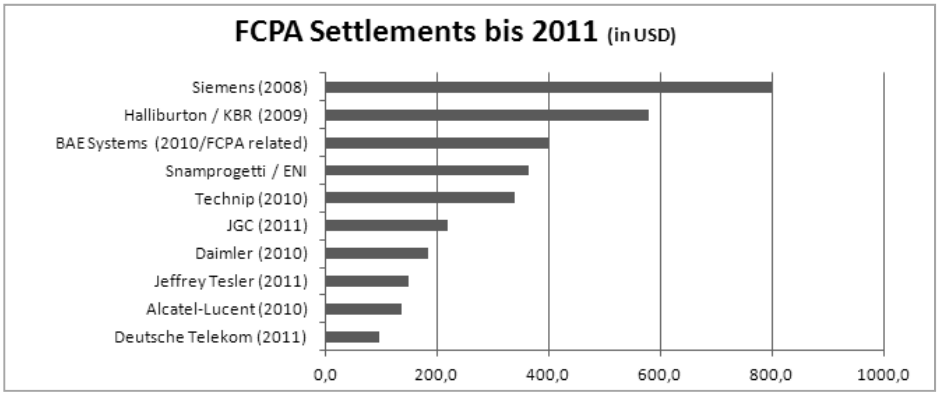

Abb. 3: Historie von TOP-FCPA Settlements bis 2011

5 Vgl. *Cassin, Richard L.* (2011), o. S.
6 Quelle: *Weissmann* (2012), o. S.

- **Australian Standard AS3806-2006 – Compliance Management**
  Der australische Standard AS3806-2006, 1998 durch Behörden, Compliance-/Ethik-Experten sowie Verbraucherschützern entwickelt, wurde erstmalig als lokale DIN-Norm in Kraft gesetzt. Somit gilt der Australian Standard als eines der ersten Rahmenwerke zur Ausgestaltung eines effektiven Compliance- und Ethik-Systems. Compliance wird hierbei in zwölf Grundprinzipien beschrieben, welche bei der Ausgestaltung des CMS berücksichtigt werden müssen:

  COMMITMENT
  - *Principle 1: Commitment by the governing body and top management to effective compliance that permeates the whole organization.*
  - *Principle 2: The compliance policy is aligned to the organization's strategy and business objectives, and is endorsed by the governing body.*
  - *Principle 3: Appropriate resources are allocated to develop, implement, maintain and improve the compliance program.*
  - *Principle 4: The objectives and strategy of the compliance program are endorsed by the governing body and top management.*
  - *Principle 5: Compliance obligations are identified and assessed.*

  IMPLEMENTATION
  - *Principle 6: Responsibility for compliant outcomes is clearly articulated and assigned.*
  - *Principle 7: Competence and training needs are identified and addressed to enable employees to fulfill their compliance obligations.*
  - *Principle 8: Behaviors that create and support compliance are encouraged and behaviors that compromise compliance are not tolerated.*
  - *Principle 9: Controls are in place to manage the identified compliance obligations and achieve desired behaviors.*

  MONITORING AND MEASURING
  - *Principle 10: Performance of the compliance program is monitored, measured and reported.*
  - *Principle 11: The organization is able to demonstrate its compliance program through both documentation and practice.*

  CONTINUAL IMPROVEMENT
  - *Principle 12: The compliance program is regularly reviewed and continually improved.*

  Compliance gliedert sich hierbei in das bestehende Risikomanagement eines Unternehmens ein. Für die Anwendung des Australian Standard existieren umfassende Materialien, die Unternehmen bei der Umsetzung unterstützen.[7, 8]

- **UK Bribery Act – Adequate procedures to prevent bribery**
  Im Jahr 2011 trat im Vereinigten Königreich der sog. UK Bribery Act in Kraft: Auf Basis des Korruptionsskandals von BAE Systems wurde eine Novellierung der Anti-Korruptionsgesetzgebung in Großbritannien angestrengt, welche in einem universel-

7 Vgl. *Standards Australia* (o.A.), o.S.
8 Vgl. *Hauschka* (2010), S. 22 ff.

len Dokument die Bestechung und Bestechlichkeit in einem nicht unerheblichen Maße sanktioniert. Die Wirkung des UK Bribery Act ist hierbei extraterritorial[9] – ebenso ist die Handlung nicht auf Amtsträger beschränkt, sondern umfasst auch den Privatsektor.

Aus Compliance-Gesichtspunkten spielen die „adeqauate proceudures to prevent bribery" eine wesentliche Rolle[10]. Diese sollen im Rahmen eines Haftungsfalles die zuvor notwendigerweise wahrgenommene Verantwortung der Organe beschreiben. So kann es sich ggfs. strafmildernd auswirken, wenn eine Unternehmung ein effektives Compliance- und Ethik-System auf Basis der „Six Principles" des UK Bribery Act installiert hatte und es sich um ein Fehlverhalten eines Individuums handelt:

Abb. 4: Die sechs Prinzipien des UK Bribery Act[11]

- **IDW PS 980 – Grundsätze ordnungsmäßiger Prüfung von Compliance-Management-Systemen**

  Neben den oben angeführten Rahmenkonzepten wurde im Jahr 2011 durch das Institut der Wirtschaftsprüfer in Deutschland der erste Prüfungsstandard zur Prüfung von Compliance-Management-Systemen veröffentlicht (IDW PS 980). Dieser Prüfungsstandard definiert im Wesentlichen die Prüfungsarten, -tiefen und die allgemeine Vorgehensweise, die ein Wirtschaftsprüfer bei der Beurteilung eines Compliance-

9 Dies bedeutet, dass die Strafverfolgung unabhängig vom Ort der Straftat erfolgen kann. So kann bei einem Unternehmen mit sog. „demonstrable business presence in the UK" ein Verfahren eingeleitet werden, wenn der Korruptionssachverhalt in einem Drittland stattgefunden hat. Für Weiteres vgl. *Ernst & Young*, Der UK Bribery Act.

10 The Bribery Act 2010 – Guidance (2011), 2 ff.

11 Quelle: *Ernst & Young*, Der UK Bribery Act (2011), S. 2.

Management-Systems als Maßstab haben soll. Die Vorgehensweise einer CMS-Prüfung wird in dem Kapitel „Compliance-Prüfungen“ tiefer gehend beschrieben. Durch den umfassenden einleitenden Teil und die Rolle des Instituts der Wirtschaftsprüfer in Deutschland setzt der Standard in der Beschreibung von Compliance-Systemen im deutschsprachigen Raum die wesentlichen Mindestanforderungen an ein solches System fest.

Im allgemeinen Teil des Standards wird das generelle Rahmenkonzept eines Compliance-Management-Systems. Hierbei stellt das IDW auf sieben Grundelemente eines effektiven Compliance- und Ethik-Systems ab, welche zwingend bei der Einrichtung eines CMS vorliegen müssen.[12]

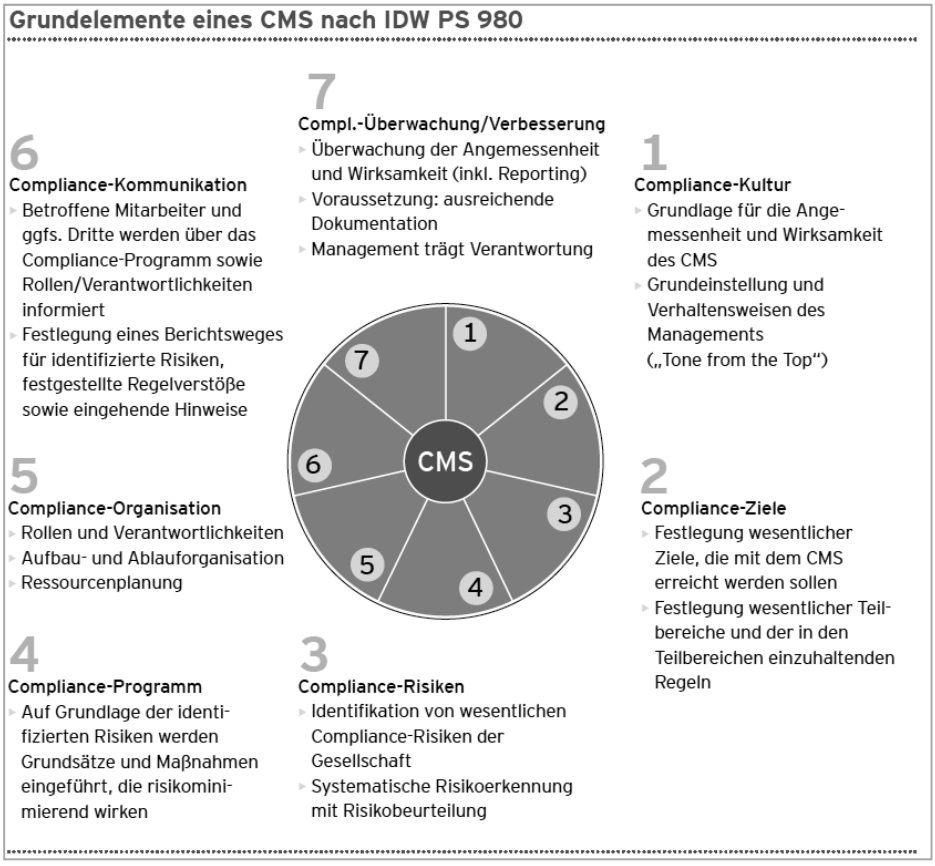

Abb. 5: Die sieben Grundelemente eines CMS nach IDW PS 980[13]

Die Relevanz zur Einrichtung von Compliance-Management-Systemen für kapitalmarktgelistete Gesellschaften wurde vom Gesetzgeber durch die Novellierung des Deut-

12 Vgl. *Institut der Wirtschaftsprüfer*, IDW PS 980, Tz. 1 ff.
13 Quelle: *Ernst & Young*, Der IDW PS 980 (2011), S. 2

schen Corporate Governance Kodex (DCGC) im Jahr 2007 verstärkt. Hier wurde im Wesentlichen auf folgende Elemente verwiesen:[14]

Deutscher Corporate Governance Kodex (Juni 2007):

Informationspflicht des Vorstands gegenüber dem Aufsichtsrat über die Compliance:

[3.4] Der Vorstand informiert den Aufsichtsrat regelmäßig, zeitnah und umfassend über alle für das Unternehmen relevanten Fragen der Planung, der Geschäftsentwicklung, der Risikolage, des Risikomanagements und der Compliance. Er geht auf Abweichungen des Geschäftsverlaufs von den aufgestellten Plänen und Zielen unter Angabe von Gründen ein;

Übernahme und Definition des Begriffes Compliance:

[4.1.3] Der Vorstand hat für die Einhaltung der gesetzlichen Bestimmungen und der unternehmensinternen Richtlinien zu sorgen und wirkt auf deren Beachtung durch die Konzernunternehmen hin (Compliance);

Pflicht des Prüfungsausschusses, sich mit Compliance zu befassen:

[5.3.2] Der Aufsichtsrat soll einen Prüfungsausschuss (Audit Committee) einrichten, der sich insbesondere mit Fragen der Rechnungslegung, des Risikomanagements und der Compliance, der erforderlichen Unabhängigkeit des Abschlussprüfers, der Erteilung des Prüfungsauftrags an den Abschlussprüfer, der Bestimmung von Prüfungsschwerpunkten und der Honorarvereinbarung befasst.

In der vorgesehenen Novellierung im Jahr 2013 wird abermals über eine Verschärfung der Governance- und Compliance-Elemente diskutiert.

Dennoch ist die Liste von allgemeinen und spezifischen Rahmenkonzepten, welche Grundlage und Ideenfundus für die Konzeption und Ausgestaltung eines Compliance-Management-Systems darstellen können, lang. Einzelne Standards stellen hier auf Branchenspezifika oder auch bestimmte Unternehmensrisiken ab. Die folgende Tabelle gibt einen Überblick über die vom Institut der Wirtschaftsprüfer in Deutschland allgemein anerkannten Rahmenkonzepte zur Ausgestaltung eines Compliance-Management-Systems:

Name	Organisation	Anwendungsbereich
1. Allgemeine Rahmenkonzepte		
Foundation Guidelines „Red Book“	Open Compliance and Ethics Group (OCEG), Phoenix, USA	Die „OCEG Guidelines“ sollen Richtlinien für die Konzeption, Implementierung, Aufrechterhaltung, Überwachung und Beurteilung von Compliance-Programmen geben. Im Vordergrund steht ein integrativer Ansatz von Governance, Compliance und Risikomanagement.

[14] Vgl. *Transparency Intl.* (2007), o.S.

Australian Standard on Compliance Programs (AS 3806-2006)	Standards Australia Committee QR-014, Sydney, Australien	Zielsetzung des AS 3806-2006 ist es, einen organisatorischen Rahmen für die Einführung und Umsetzung wirksamer Compliance-Programme zu geben.
Unternehmensweites Risikomanagement – Übergreifendes Rahmenwerk (COSO II)	Committee of Sponsoring Organization, Jersey City, USA	Umfassendes Modell eines unternehmensweiten Risikomanagements
OECD-Grundsätze der Corporate Governance	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD), Paris, Frankreich	Grundsätze der OECD für Corporate Governance, die weltweit Mindeststandards setzen sollen
OECD Guidelines for Multinational Enterprises	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD), Paris, Frankreich	Die OECD-Leitsätze für multinationale Unternehmen stellen Empfehlungen für ein verantwortungsvolles und dem geltenden Recht entsprechendes unternehmerisches Verhalten dar.
2. Spezifische Rahmenkonzepte		
Pflichtenheft zum Compliance-Management in der Immobilienwirtschaft	Initiative Corporate Governance der deutschen Immobilienwirtschaft e.V., Berlin	Grundsätze für eine transparente und professionelle Unternehmensführung in der Immobilienwirtschaft
Grundsätze ordnungsmäßiger Compliance	Österreichische Finanzmarktaufsicht, Wien, Österreich	Grundsätze ordnungsmäßiger Compliance für österreichische Kreditinstitute, die Geschäfte und Dienstleistungen im Zusammenhang mit Finanzinstrumenten durchführen
United States Federal Sentencing Guidelines Manual	United States Sentencing Commission	US-Grundsätze für organisatorische Maßnahmen zur Verhinderung von Straftaten der Mitglieder einer Organisation bzw. zur Mitwirkung bei der Aufdeckung von Straftaten

PACI: Principles for Countering Bribery	Partnering Against Corruption Initiative (PACI), Genf, Schweiz	Prinzipien zur Verhinderung von Bestechung
OFT Guide for Compliance with Competition Law	Office of fair trading (OFT), London, England (non-ministerial government department in UK)	Grundsätze zur Einhaltung von Vorschriften des Wettbewerbsrechts
Korruption bekämpfen – Ein ICC-Verhaltenskodex für die Wirtschaft	ICC Deutschland e.V., Internationale Handelskammer, Berlin / Deutscher Industrie- und Handelskammertag e.V., Berlin	Verhaltenskodex zur Korruptionsbekämpfung
Geschäftsgrundsätze für die Bekämpfung von Korruption	Transparency International Deutschland e.V., Berlin	Geschäftsgrundsätze für die Bekämpfung von Korruption
BME-Verhaltensrichtlinie Code of Conduct	Bundesverband für Materialwirtschaft, Einkauf und Logistik e.V., Frankfurt/ Main	Die BME-Verhaltensrichtlinie ist ein freiwilliger Kodex zur Umsetzung von nachhaltigen, verantwortungsvollen und ethischen Handlungsgrundsätzen.
Consultation on Guidance about commercial organisations preventing bribery (Guidance to the UK Bribery Act)	The Ministry of Justice, London	Zum „UK Bribery Act“ sind Richtlinien vorgesehen (am 14.09.2010 als Entwurf veröffentlicht), die den Unternehmen helfen sollen, die Anforderungen des UK Bribery Act zu erfüllen. Der „UK Bribery Act“ ist ein Antikorruptionsgesetz, das Bestechungstaten unter Strafe stellt. Auch deutsche Unternehmen können in den Anwendungsbereich des Gesetzes fallen, wenn sie einen hinreichenden Geschäftsbezug zu Großbritannien (z.B. durch eine Betriebsstätte oder umfangreiche Warenlieferungen) haben.

Recommendation of the Council for Further Combating Bribery of Foreign Public Officials in International Business Transactions; Annex II: Good Practice Guidance on Internal Controls, Ethics, and Compliance	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD), Paris, Frankreich	Die Leitlinien richten sich an Unternehmen mit dem Ziel, die Wirksamkeit von Programmen oder Maßnahmen in den Gebieten Interner Kontrollsysteme, Ethik und Compliance mit dem Zweck der Verhütung und Aufklärung von Bestechung ausländischer Amtsträger im internationalen Geschäftsverkehr sicherzustellen.

Abb. 6: Allgemeine und spezifische Rahmenkonzepte nach IDW PS 980[15]

1.3. CMS-Risiken und Anwendungsbereich

Wie bereits in der Definition eines CMS angeführt, zielt das Management-System auf die systematische Verhinderung von Fehlverhalten bezogen auf das individuelle, für das Unternehmen geltende Risiko ab. Welches Risiko jedoch für ein Unternehmen ein wesentliches Risiko darstellt, ist nicht pauschal zu beantworten. In der Vergangenheit haben Industrie-Compliance-Systeme meist Kernrisiken im Bereich Anti-Korruption abgedeckt. Aber auf Basis zunehmender Internationalisierung und Regulierung von Erwartungen der Stakeholder an eine Good Governance and Citizenship hat sich auch das allgemeine Risikoportfolio im Bereich Compliance verändert.

Prinzipiell ist erst einmal festzustellen, dass einzelne Industrien und Branchen durch die Geschäftsmodelle per se regulatorische Compliance-Risiken abzudecken haben:

Finanzdienstleistungsbranche (Banken, Versicherungen etc.):
Die Finanzdienstleistungsbranche ist auf Basis ihrer öffentlichen Stellung und volkswirtschaftlicher Relevanz von lokalen Gesetzgebern an sich stark reguliert. In der Regel greifen nationale Kapitalmarkt-/Finanzdienstleistungs-Gesetze und Standards sowie spezifische Transparenz- und Überwachungselemente.

Medizin, Pharmazie, Health Care (Life Science):
Der Bereich „Life Science" hat in der Vergangenheit stets eine hohe Dichte an Regulierung erfahren müssen. Gerade auf Basis des hohen Risikos eines möglichen Haftungsfalles durch gesundheitliche Schäden o.Ä. kam es zur Einführung nationaler und internationaler Standards und Regularien, welche mittelbare Auswirkung auf die Ausgestaltung eines unternehmensspezifischen CMS haben.

Oil & Gas/Energy:
Ähnlich wie im Bereich „Life Science" konnte im Bereich Energie, Oil and Gas eine hohe Regulierung festgestellt werden. Zur Sicherstellung von – weitestgehend nationa-

[15] Quelle: *Institut der Wirtschaftsprüfer*, IDW PS 980, Anlage 1.