

Entwurf IDW Prüfungsstandard: Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen (IDW EPS 980)

(Stand: 11.03.2010)¹

Der Hauptfachausschuss (HFA) des IDW hat den nachfolgenden Entwurf des IDW Prüfungsstandards: Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen verabschiedet.

Eventuelle Änderungs- oder Ergänzungsvorschläge zu dem Entwurf werden schriftlich an die Geschäftsstelle des IDW, Postfach 32 05 80, 40420 Düsseldorf, bis zum 01.10.2010 erbeten. Die Änderungs- oder Ergänzungsvorschläge werden im Internet auf der IDW Homepage veröffentlicht, wenn dies nicht ausdrücklich vom Verfasser abgelehnt wird.

Der Entwurf steht bis zu seiner endgültigen Verabschiedung als IDW Prüfungsstandard im Internet (www.idw.de) unter der Rubrik Verlautbarungen als Download-Angebot zur Verfügung.

Copyright © Institut der Wirtschaftsprüfer in Deutschland e.V., Düsseldorf.

1.	Vorbemerkungen.....	2
2.	Begriffsbestimmungen.....	3
3.	Gegenstand, Ziel und Umfang der Prüfung	4
4.	Grundelemente eines CMS	5
5.	Prüfungsanforderungen.....	7
5.1.	Berufspflichten	7
5.2.	Auftragsannahme.....	7
5.3.	Prüfungsplanung.....	8
5.3.1.	Allgemeine Grundsätze.....	8
5.3.2.	Wesentlichkeit.....	9
5.4.	Prüfungsdurchführung.....	9
5.4.1.	Prüfungshandlungen zur Risikobeurteilung.....	9
5.4.1.1.	Kenntnisse über das rechtliche und wirtschaftliche Umfeld des Unternehmens	9
5.4.1.2.	Konzeption des CMS (Auftragstypen 1, 2 und 3).....	9
5.4.2.	Aufbau- und Funktionsprüfung des CMS (Auftragstypen 2 und 3).....	10
5.4.3.	Weitere Prüfungshandlungen.....	10
5.4.3.1.	Festgestellte Regelverstöße	10
5.4.3.2.	Verwertung der Arbeit von Spezialisten	11
5.4.3.3.	Ereignisse bis zum Datum der Berichterstattung über die CMS-Prüfung	11

¹ Verabschiedet vom Hauptfachausschuss (HFA) am 11.03.2010.

5.4.3.4.	Vollständigkeitserklärung	11
5.4.4.	Auswertung der Prüfungsfeststellungen und Ableitung des Prüfungsurteils.....	12
5.5.	Dokumentation.....	13
5.6.	Berichterstattung des CMS-Prüfers.....	13
5.6.1.	CMS-Prüfungsbericht.....	13
5.6.2.	Weitere Berichtspflichten	15
6.	Anwendungshinweise und Erläuterungen.....	15
	Anlagen.....	29
1.	Allgemein anerkannte CMS-Rahmenkonzepte	29
2.	Berichterstattung über CMS-Prüfungen.....	31
2.1.	Auftragstyp 1	31
2.2.	Auftragstyp 2.....	34
2.3.	Auftragstyp 3.....	38
2.4.	Auftragstyp 3 mit Einschränkung.....	41

1. Vorbemerkungen

- 1 Das Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW) verdeutlicht in diesem *IDW Prüfungsstandard* den Inhalt freiwilliger Prüfungen von Compliance Management Systemen (CMS-Prüfungen) und legt die Berufsauffassung dar, nach der Wirtschaftsprüfer unbeschadet ihrer Eigenverantwortlichkeit derartige Aufträge durchführen (vgl. Tz. A1). Als Teilbereich des unternehmensweiten Risikomanagements ist das Compliance Management System (CMS) auf die Einhaltung von Regeln im Unternehmen ausgerichtet. Sofern in diesem Prüfungsstandard die Begriffe „CMS“ oder „CMS-Prüfung“ verwendet werden, beziehen sich diese auf die von den gesetzlichen Vertretern bestimmten Teilbereiche des CMS (vgl. Tz. A2).

Der *IDW Prüfungsstandard* enthält in Abschn. 5 verpflichtend zu beachtende Prüfungsanforderungen sowie in Abschn. 6 Anwendungshinweise und Erläuterungen zu den Prüfungsanforderungen.
- 2 Der *IDW Prüfungsstandard* ist nicht anzuwenden auf Prüfungen von Systemen, für die spezielle *IDW Prüfungsstandards* bestehen, z.B. auf die Prüfung von Risikofrüherkennungssystemen i.S.d. *IDW PS 340*² oder die Prüfung von Risikomanagementsystemen i.S.d. *IDW EPS 525*³.
- 3 Dieser *IDW Prüfungsstandard* ist erstmals anzuwenden bei CMS-Prüfungen, die nach dem [30.06.2011] durchgeführt werden.
- 4 Dieser *IDW Prüfungsstandard* steht im Einklang mit dem International Framework for Assurance Engagements und dem International Standard on Assurance Engagements.

² *IDW Prüfungsstandard: Die Prüfung des Risikofrüherkennungssystems nach § 317 Abs. 4 HGB (IDW PS 340)* (Stand: 11.09.2000).

³ *Entwurf IDW Prüfungsstandard: Die Beurteilung des Risikomanagements von Kreditinstituten im Rahmen der Abschlussprüfung (IDW EPS 525)* (Stand: 06.03.2009).

gements (ISAE) 3000 „Assurance Engagements other than Audits or Reviews of Historical Financial Information“.⁴

2. Begriffsbestimmungen

- 5 Unter dem Begriff *Compliance* ist allgemein die Einhaltung von Regeln zu verstehen (z.B. Gesetze, vertragliche Verpflichtungen und interne Regelungen oder Richtlinien).
- 6 Unter einem *Compliance Management System* sind die auf der Grundlage der von den gesetzlichen Vertretern festgelegten Ziele (vgl. Tz. 19) eingeführten Grundsätze und 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, d.h. auf die Einhaltung bestimmter Regeln bzw. die Verhinderung von wesentlichen Verstößen (Regelverstöße) (vgl. Tz. A3). Ein CMS i.S.d. *IDW Prüfungsstandards* kann sich u.a. auf Geschäftsbereiche, auf operative Prozesse (z.B. den Einkauf) oder auf bestimmte Rechtsgebiete (z.B. Kartellrecht) beziehen (abgegrenzte Teilbereiche) (vgl. Tz. A2).
- 7 Bei den *Aussagen der gesetzlichen Vertreter* des Unternehmens über das CMS handelt es sich um in einer CMS-Beschreibung explizit oder implizit enthaltene Erklärungen zur Konzeption des CMS, zu den Grundelementen des CMS sowie zur Angemessenheit, Implementierung und Wirksamkeit des CMS in Übereinstimmung mit den angewandten CMS-Grundsätzen.
- 8 Unter *CMS-Grundsätzen* sind allgemein anerkannte Rahmenkonzepte, andere angemessene Rahmenkonzepte oder vom Unternehmen selbst entwickelte Grundsätze für Compliance Management Systeme zu verstehen (vgl. Tz. A26).
- 9 Unter *allgemein anerkannten Rahmenkonzepten* für CMS sind solche Rahmenkonzepte zu verstehen, die von einer autorisierten oder anerkannten standardsetzenden Organisation im Rahmen eines transparenten Verfahrens entwickelt und verabschiedet oder durch gesetzliche oder andere rechtliche Anforderungen festgelegt werden (vgl. Tz. A4 und Anlage 1).
- 10 Die *Konzeption eines CMS* umfasst die Förderung einer günstigen Compliance-Kultur sowie die Festlegung der Compliance-Ziele, den Aufbau der Compliance-Organisation (Aufbau- und Ablauforganisation), den Prozess der Feststellung und Analyse der Compliance-Risiken durch das Unternehmen, den Prozess der Erstellung des Compliance-Programms, die Entwicklung eines Kommunikationsprozesses sowie von Verfahren zur Überwachung und Verbesserung des CMS.
- 11 Eine *CMS-Beschreibung* beinhaltet unter Berücksichtigung der angewandten CMS-Grundsätze eine Darstellung zu sämtlichen Grundelementen eines CMS (vgl. Tz. 19). Die angewandten CMS-Grundsätze sind dabei in der CMS-

⁴ Vgl. IFAC, Handbook of International Standards on Auditing, Assurance, and Ethics Pronouncements, New York 2008, Part I, S. 188 ff. und 922 ff.

Beschreibung entweder durch Verweis auf allgemein zugängliche CMS-Grundsätze oder durch Aufzählung der einzelnen Grundsätze zu konkretisieren. Die CMS-Beschreibung beinhaltet in Abhängigkeit vom Auftragsstyp explizite oder implizite Aussagen der gesetzlichen Vertreter zu Art, Umfang und Zeitpunkt der Konzeption des CMS bzw. zur Angemessenheit, Implementierung und Wirksamkeit des CMS zu einem bestimmten Zeitpunkt bzw. in einem bestimmten Zeitraum.

3. Gegenstand, Ziel und Umfang der Prüfung

- 12 Gegenstand der Prüfung sind die in einer CMS-Beschreibung enthaltenen Aussagen der gesetzlichen Vertreter über das CMS.
- 13 Die Verantwortung für das CMS und die CMS-Beschreibung liegt bei den gesetzlichen Vertretern des Unternehmens. Diese Verantwortung umfasst auch die Dokumentation des CMS, um eine konsistente Anwendung und personenunabhängige Funktion des Systems im Zeitablauf zu ermöglichen sowie die Organisation der Erstellung der CMS-Beschreibung durch geeignete Personen, z.B. den Compliance-Beauftragten (vgl. Tz. A5 f.).
- 14 Ziel einer CMS-Prüfung ist es, dem Prüfer anhand der festgelegten Kriterien eine Aussage mit hinreichender Sicherheit darüber zu ermöglichen (vgl. Tz. A7), ob
- a) die Aussagen der gesetzlichen Vertreter in der CMS-Beschreibung zur Konzeption des CMS in allen wesentlichen Belangen zutreffend dargestellt sind und die CMS-Beschreibung auf sämtliche der in Tz. 19 genannten Grundelemente eines CMS eingeht (Auftragsstyp 1) (vgl. Tz. 10) oder
 - b) die Aussagen der gesetzlichen Vertreter in der CMS-Beschreibung über die Grundsätze und Maßnahmen des CMS in allen wesentlichen Belangen zutreffend dargestellt sind, dass die dargestellten Grundsätze und Maßnahmen in Übereinstimmung mit den angewandten CMS-Grundsätzen geeignet sind, Risiken für wesentliche Regelverstöße mit hinreichender Sicherheit rechtzeitig zu erkennen und Verstöße zu verhindern und dass die Grundsätze und Maßnahmen zu einem bestimmten Zeitpunkt implementiert sind (Auftragsstyp 2), oder
 - c) die Aussagen der gesetzlichen Vertreter in der CMS-Beschreibung über die Grundsätze und Maßnahmen des CMS in allen wesentlichen Belangen zutreffend dargestellt sind, dass die dargestellten Grundsätze und Maßnahmen in Übereinstimmung mit den angewandten CMS-Grundsätzen geeignet sind, Risiken für wesentliche Regelverstöße mit hinreichender Sicherheit rechtzeitig zu erkennen und Verstöße zu verhindern und dass die Grundsätze und Maßnahmen zu einem bestimmten Zeitpunkt implementiert sind und während eines bestimmten Zeitraums wirksam waren (Auftragsstyp 3).
- 15 Der CMS-Prüfer hat die Beschreibung der Konzeption des CMS im Rahmen seiner Beurteilung des Risikos wesentlicher Fehler in den Aussagen der gesetzlichen Vertreter auch bei den Auftragsstypen 2 und 3 zu beurteilen. Dies schließt nicht aus, mit dem Auftraggeber in einem Auftrag des Auftragsstyps 1 zu vereinbaren, dass der

CMS-Prüfer die Beschreibung der Konzeption des CMS separat beurteilt und darüber einen Bericht erstellt.

- 16 Ein CMS ist angemessen, wenn es mit hinreichender Sicherheit gewährleistet, dass Risiken für wesentliche Verstöße gegen die betreffenden Regeln rechtzeitig erkannt und Verstöße verhindert werden. Zu einem angemessenen CMS zählt auch, dass bereits eingetretene Verstöße an die zuständige Stelle im Unternehmen zu berichten sind, damit die notwendigen Konsequenzen für eine Verbesserung des CMS getroffen werden (vgl. Tz. A8).

Der Begriff Implementierung bezieht sich auf die Einführung der Grundsätze und Maßnahmen des CMS in die Geschäftsprozesse und nicht auf die Wirksamkeit der Grundsätze und Maßnahmen in den laufenden Geschäftsprozessen.

- 17 Die Wirksamkeit des CMS ist dann gegeben, wenn die Grundsätze und Maßnahmen von den hiervon Betroffenen nach Maßgabe ihrer Verantwortung zur Kenntnis genommen und beachtet werden (vgl. Tz. A8 f.).
- 18 Es liegt in der Verantwortung des CMS-Prüfers, Prüfungshandlungen durchzuführen, um ausreichende und angemessene Prüfungsnachweise zu erlangen, auf die er sein Urteil zu den in der CMS-Beschreibung enthaltenen Aussagen der gesetzlichen Vertreter stützen kann.

4. Grundelemente eines CMS

- 19 Ein angemessenes CMS i.S.d. *IDW Prüfungsstandards* weist die folgenden miteinander in Wechselwirkung stehenden Grundelemente auf, die in die Geschäftsabläufe eingebunden sind. Bei der Konzeption des CMS sind die Wechselwirkungen zwischen den Grundelementen zu berücksichtigen (vgl. Tz. A10 ff.):

Compliance-Kultur	Die Compliance-Kultur stellt die Grundlage für die Angemessenheit und Wirksamkeit des CMS dar. Sie wird vor allem geprägt durch die Grundeinstellungen und Verhaltensweisen des Managements sowie durch die Rolle des Aufsichtsorgans („tone at the top“). Die Compliance-Kultur beeinflusst die Bedeutung, welche die Mitarbeiter des Unternehmens der Beachtung von Regeln beimessen und damit die Bereitschaft zu regelkonformem Verhalten.
-------------------	--

Compliance-Ziele	Die gesetzlichen Vertreter legen auf der Grundlage der allgemeinen Unternehmensziele und einer Analyse und Gewichtung der für das Unternehmen bedeutsamen Regeln die Ziele fest, die mit dem CMS erreicht werden sollen. Dies umfasst insb. die Festlegung der relevanten Teilbereiche und der in den einzelnen Teilbereichen einzuhaltenden Regeln. Die Compliance-Ziele stellen die Grundlage für die Beurteilung von Compliance-Risiken dar.
Compliance-Organisation	Das Management regelt die Rollen und Verantwortlichkeiten (Aufgaben) sowie Aufbau- und Ablauforganisation im CMS als integralen Bestandteil der Unternehmensorganisation und stellt die für ein wirksames CMS notwendigen Ressourcen zur Verfügung.
Compliance-Risiken	Unter Berücksichtigung der Compliance-Ziele werden die Compliance-Risiken festgestellt, die Verstöße gegen einzuhaltende Regeln und damit eine Verfehlung der Compliance-Ziele zur Folge haben können. Hierzu wird ein Verfahren zur systematischen Risikoerkennung und -berichterstattung eingeführt. Die festgestellten Risiken werden im Hinblick auf Eintrittswahrscheinlichkeit und mögliche Folgen (z.B. Schadenshöhe) analysiert.
Compliance-Programm	Auf der Grundlage der Beurteilung der Compliance-Risiken werden Grundsätze und Maßnahmen eingeführt, die auf die Begrenzung der Compliance-Risiken und damit auf die Vermeidung von Compliance-Verstößen ausgerichtet sind. Das Compliance-Programm umfasst auch die bei festgestellten Compliance-Verstößen zu ergreifenden Maßnahmen. Das Compliance-Programm wird zur Sicherstellung einer personenunabhängigen Funktion des CMS dokumentiert.
Compliance-Kommunikation	Die jeweils betroffenen Mitarbeiter und ggf. Dritte werden über das Compliance-Programm sowie die festgelegten Rollen und Verantwortlichkeiten informiert, damit diese ihre Aufgaben im CMS ausreichend verstehen und sachgerecht erfüllen können. Im Unternehmen wird festgelegt, wie Compliance-Risiken sowie Hinweise auf mögliche und festgestellte Regelverstöße an die zuständigen Stellen im Unternehmen (z.B. den Compliance-Beauftragten, die gesetzlichen Vertreter und erforderlichenfalls das Aufsichtsorgan) berichtet werden.

Compliance-Überwachung und Verbesserung	Die Angemessenheit und Wirksamkeit des CMS werden in geeigneter Weise überwacht. Voraussetzung für die Überwachung ist eine ausreichende Dokumentation des CMS. Werden im Rahmen der Überwachung Schwachstellen im CMS bzw. Verstöße festgestellt, werden diese an das Management bzw. die hierfür bestimmte Stelle im Unternehmen berichtet. Die gesetzlichen Vertreter sorgen für die Durchsetzung des CMS, die Beseitigung der Mängel und die Verbesserung des Systems.
---	--

5. Prüfungsanforderungen

5.1. Berufspflichten

20 Bei CMS-Prüfungen handelt es sich um betriebswirtschaftliche Prüfungen, bei denen neben den allgemeinen Berufspflichten der Unabhängigkeit, Verschwiegenheit, Eigenverantwortlichkeit und Gewissenhaftigkeit (§§ 17 Abs. 1, 43 Abs. 1 Satz 1, 49 WPO, §§ 1 – 9 BS WP/vBP) auch die besonderen Berufspflichten nach §§ 20 – 27a BS WP/vBP zu beachten sind.

5.2. Auftragsannahme

21 Ein Auftrag zur Durchführung einer CMS-Prüfung darf nur angenommen werden, wenn die Berufspflichten einschließlich des Unabhängigkeitsgrundsatzes eingehalten werden können.⁵ Dies setzt u.a. voraus, dass ausreichende Erfahrung und Kompetenz sowie personelle und zeitliche Ressourcen in der WP-Praxis vorhanden sind, um den Auftrag ordnungsgemäß durchführen zu können (§ 4 Abs. 2 BS WP/vBP).

22 Bei der notwendigen Beurteilung der Auftragsrisiken vor Auftragsannahme ist insb. festzustellen, ob die für die Durchführung des Auftrags notwendigen Fach- und Branchenkenntnisse verfügbar sind, Erfahrungen mit den einschlägigen rechtlichen Anforderungen vorliegen oder erlangt werden können und erforderlichenfalls Spezialisten zur Verfügung stehen.⁶

23 Im Zusammenhang mit der Entscheidung über die Annahme einer CMS-Prüfung hat sich der Wirtschaftsprüfer Informationen über die Ausgestaltung des CMS und der angewandten CMS-Grundsätze zu verschaffen, um die grundsätzliche Eignung des in der CMS-Beschreibung dargestellten Systems als Prüfungsgegenstand zu beurteilen. Diese Beurteilung hat anhand der in Tz. 19 dargestellten Grundelemente eines CMS zu erfolgen (vgl. Tz. A17).

⁵ Vgl. *Gemeinsame Stellungnahme der WPK und des IDW: Anforderungen an die Qualitätssicherung in der Wirtschaftsprüferpraxis (VO 1/2006)* (Stand: 27.03.2006).

⁶ Vgl. *VO 1/2006*, Tz. 61.

- 24 Da Grundlage der Prüfung eine Beschreibung des im Unternehmen eingerichteten CMS ist, darf der Prüfer den Auftrag nur annehmen, wenn eine CMS-Beschreibung der gesetzlichen Vertreter vorliegt bzw. die gesetzlichen Vertreter ihre Bereitschaft erklären, eine CMS-Beschreibung zu erstellen.
- 25 Der Prüfer hat mit dem Auftraggeber die Auftragsbedingungen schriftlich zu vereinbaren (vgl. Tz. A18 f.).
- 26 In den Auftragsbedingungen ist darauf hinzuweisen, dass keine Prüfungssicherheit über die tatsächliche Einhaltung von Regeln erlangt wird, sondern ausschließlich die von den gesetzlichen Vertretern in der CMS-Beschreibung getroffenen Aussagen zum CMS beurteilt werden.

5.3. Prüfungsplanung

5.3.1. Allgemeine Grundsätze

- 27 Der CMS-Prüfer hat die Prüfung in sachlicher, personeller und zeitlicher Hinsicht so zu planen, dass eine ordnungsgemäße Prüfungsdurchführung gewährleistet ist.
- 28 Bei der Auswahl der Mitglieder des Prüfungsteams ist darauf zu achten, dass ausreichende praktische Erfahrungen mit Systemprüfungen sowie die notwendigen Branchen- und Rechtskenntnisse vorhanden sind (§ 24a Abs. 3 BS WP/vBP). Das Prüfungsteam muss über ausreichende Kenntnisse der Anforderungen verfügen, auf deren Einhaltung das CMS abzielt. Erforderlichenfalls sind Spezialisten hinzuzuziehen, z.B. wenn Aussagen der gesetzlichen Vertreter über die Angemessenheit des CMS zur Verhinderung wirtschaftskrimineller Handlungen oder zur Einhaltung komplexer regulatorischer Anforderungen zu beurteilen sind.
- 29 Der Prüfer muss die Prüfungshandlungen mit einer kritischen Grundhaltung⁷ so planen und durchführen, dass das Prüfungsrisiko soweit reduziert wird, dass mit hinreichender Sicherheit beurteilt werden kann, ob die Aussagen der gesetzlichen Vertreter in der CMS-Beschreibung keine wesentlichen Fehler enthalten.
- 30 Bei dem Prüfungsrisiko handelt es sich um das Risiko, dass der Prüfer ein uneingeschränktes Prüfungsurteil abgibt, wenn die Aussagen der gesetzlichen Vertreter in der CMS-Beschreibung einen wesentlichen Fehler aufweisen.
- 31 Der Prüfer muss die geplanten Prüfungshandlungen in einem Prüfungsprogramm zusammenfassen, das die Prüfungsanweisungen zur sachlichen und zeitlichen Auftragsabwicklung für die Mitglieder des Prüfungsteams enthält (§ 24a Abs. 1 BS WP/vBP).
- 32 Zudem sind die übrigen auftragsbezogenen Qualitätssicherungsmaßnahmen zu planen. Hierbei handelt es sich insb. um die Überwachung der Auftragsabwicklung,

⁷ Zur kritischen Grundhaltung vgl. *IDW Prüfungsstandard: Ziele und allgemeine Grundsätze der Durchführung von Abschlussprüfungen (IDW PS 200)* (Stand: 28.06.2000), Tz. 17.

die Durchsicht der Prüfungsergebnisse und – bei Vorliegen der Voraussetzungen – die Berichtskritik bzw. die auftragsbegleitende Qualitätssicherung.

5.3.2. Wesentlichkeit

- 33 Der CMS-Prüfer hat für Zwecke der Planung und Durchführung der Prüfungshandlungen sowie der Auswertung der Prüfungsergebnisse zu bestimmen, in welchen Fällen ein Fehler in den Aussagen der gesetzlichen Vertreter in der CMS-Beschreibung als wesentlich einzustufen ist (vgl. Tz. A20 ff.).
- 34 Die Bestimmung der Wesentlichkeit von (möglichen) Verstößen liegt im prüferischen Ermessen des CMS-Prüfers. Hierbei sind insb. die Bedeutung der verletzten Regel, die Folgen des Verstoßes, die Motivation für den Verstoß sowie die Tragweite des Verstoßes zu berücksichtigen (vgl. Tz. A23).

5.4. Prüfungsdurchführung

- 35 Der Prüfer hat Prüfungshandlungen zur Feststellung von Risiken für wesentliche Fehler in den Aussagen der gesetzlichen Vertreter in der CMS-Beschreibung durchzuführen. Die festgestellten Risiken stellen die Grundlage für die weiteren Prüfungshandlungen zur Beurteilung der Aussagen der gesetzlichen Vertreter in der CMS-Beschreibung dar (vgl. Tz. A24).

5.4.1. Prüfungshandlungen zur Risikobeurteilung

5.4.1.1. Kenntnisse über das rechtliche und wirtschaftliche Umfeld des Unternehmens

- 36 Zur Feststellung des Risikos, dass die Aussagen der gesetzlichen Vertreter in der CMS-Beschreibung wesentliche Fehler aufweisen, hat sich der Prüfer mit dem rechtlichen und wirtschaftlichen Umfeld, den Merkmalen des Unternehmens sowie den Unternehmenszielen und -strategien zu befassen, soweit sie für den bzw. die zu prüfenden Teilbereich(e) des CMS relevant ist/sind (vgl. Tz. A25).

5.4.1.2. Konzeption des CMS (Auftragstypen 1, 2 und 3)

- 37 Der CMS-Prüfer hat die Aussagen der gesetzlichen Vertreter in der CMS-Beschreibung zur Konzeption des CMS im Rahmen der Feststellung und Analyse der Risiken für wesentliche Fehler zu beurteilen (Auftragstypen 2 und 3). Bei den Auftragstypen 2 und 3 ist die Beschreibung der Konzeption des CMS kein separater Prüfungsgegenstand, sondern Ausgangspunkt für die risikoorientierte Festlegung weiterer Prüfungshandlungen.
- 38 Beim Auftragsstyp 1 hat der CMS-Prüfer zu beurteilen, ob die Aussagen der gesetzlichen Vertreter in der CMS-Beschreibung zur Konzeption des CMS zutreffend sind und die Beschreibung auf sämtliche der in Tz. 19 genannten Grundelemente eines CMS eingeht. In diesem Fall ist die Beschreibung der Konzeption des CMS selbst

Prüfungsgegenstand der CMS-Prüfung, zu dem der CMS-Prüfer ein Prüfungsurteil erteilt (vgl. Tz. A26).

- 39 Bei der Bestimmung von Art und Umfang der Prüfungshandlungen sind die angewandten CMS-Grundsätze, die Beschreibung des CMS durch die gesetzlichen Vertreter und die der Prüfung unterliegenden Teilbereiche des CMS zu berücksichtigen (vgl. Tz. A27).

5.4.2. Aufbau- und Funktionsprüfung des CMS (Auftragstypen 2 und 3)

- 40 Der Prüfer hat die Ergebnisse seiner Risikobeurteilungen zu analysieren und bei den weiteren Prüfungshandlungen zu berücksichtigen. Wenn dem Prüfer bereits anlässlich der Prüfungshandlungen zur Beurteilung der Konzeption des CMS (vgl. Tz. 37 ff.) erhebliche Mängel bekannt werden, kann er zu dem Ergebnis gelangen, dass das CMS nicht angemessen ausgestaltet ist. In diesem Fall erübrigen sich weitere Prüfungshandlungen zur Aufbau- und Funktionsprüfung des CMS.
- 41 Im Rahmen der Aufbauprüfung des CMS hat der Prüfer zu beurteilen, ob die in der CMS-Beschreibung des Unternehmens dargestellten Grundsätze und Maßnahmen so ausgestaltet und implementiert sind, dass Risiken für wesentliche Regelverstöße mit hinreichender Sicherheit rechtzeitig erkannt und Verstöße verhindert werden (vgl. Tz. A28 f.).
- 42 Die Funktionsprüfung des CMS zielt zusätzlich auf die Beurteilung ab, ob die in der CMS-Beschreibung dargestellten Grundsätze und Maßnahmen innerhalb eines bestimmten Zeitraums wirksam waren (vgl. Tz. A30).
- 43 Die Beurteilung der Kontinuität der Beachtung der Regelungen des CMS erfordert es, dass die Funktionsprüfung einen angemessenen Zeitraum abdeckt, z.B. ein Geschäftsjahr. Die gewonnene Prüfungssicherheit in Bezug auf die Wirksamkeit des CMS ist bei gleicher Prüfungsintensität um so größer, je länger der geprüfte Zeitraum ist. Sofern Prüfungshandlungen zur Beurteilung der Wirksamkeit der Grundsätze und Maßnahmen zu einem vorgezogenen Zeitpunkt durchgeführt werden, hat der Prüfer festzulegen, welche Prüfungsnachweise zur Beurteilung der Wirksamkeit für den Zeitraum bis zum Ende des zu prüfenden Zeitraums einzuholen sind.

5.4.3. Weitere Prüfungshandlungen

5.4.3.1. Festgestellte Regelverstöße

- 44 Stellt der Prüfer anlässlich seiner Prüfungstätigkeit Regelverstöße fest oder liegen ihm entsprechende Anhaltspunkte vor, hat er die verantwortlichen Mitglieder des Managements und ggf. die gesetzlichen Vertreter darüber zu informieren. Bei festgestellten Regelverstößen liegt es in der Verantwortung der gesetzlichen Vertreter zu untersuchen, welche Umstände zu dem Verstoß geführt haben und warum das CMS den Verstoß nicht verhindert hat.

- 45 Der Prüfer hat sich mit der Untersuchung und den Untersuchungsergebnissen des Unternehmens zu befassen und eigenverantwortlich zu beurteilen, ob festgestellte Regelverstöße auf Mängel im CMS zurückzuführen sind. Ohne entsprechende Prüfungsnachweise kann der Prüfer nicht davon ausgehen, dass es sich bei dem Regelverstoß um einen einmaligen Vorgang handelt.

5.4.3.2. Verwertung der Arbeit von Spezialisten

- 46 Wenn bedeutsame Sachverhalte vom Prüfungsteam allein nicht beurteilt werden können, sind Spezialisten hinzuzuziehen (vgl. Tz. A33).
- 47 Beim Einsatz interner Spezialisten des Prüfers sind diese Gegenstand des Qualitätssicherungssystems der WP-Praxis. Es ist seine Aufgabe, die internen Spezialisten angemessen anzuleiten und zu überwachen.
- 48 Plant der CMS-Prüfer die Verwertung von Arbeiten externer Spezialisten, muss er sich über deren berufliche Qualifikation und fachliche Kompetenz informieren. Zudem muss er den Grad der Unabhängigkeit der Spezialisten vom zu prüfenden Unternehmen berücksichtigen.
- 49 Der Prüfer hat sich mit dem Arbeitsauftrag der externen Spezialisten zu befassen und die auf dieser Grundlage durchgeführten Arbeiten zu beurteilen (Ausgangsdaten, Annahmen, Methoden und Ergebnisse) (vgl. Tz. A34).

5.4.3.3. Ereignisse bis zum Datum der Berichterstattung über die CMS-Prüfung

- 50 Der Prüfer hat die Auswirkungen von Ereignissen nach dem in der CMS-Beschreibung genannten Zeitpunkt/Zeitraum, auf den sich die Aussagen der gesetzlichen Vertreter beziehen, bis zum Datum seiner Berichterstattung zu würdigen (vgl. Tz. A35).
- 51 Falls dem CMS-Prüfer nach dem Datum der Berichterstattung über die CMS-Prüfung bis zur Auslieferung der Berichterstattung Sachverhalte bekannt werden, die auf Mängel im CMS hindeuten oder bei denen es sich um Verstöße oder vermutete Verstöße handeln kann, hat er die Adressaten der Berichterstattung hierüber zu informieren. Der Prüfer hat in diesem Fall zu untersuchen, ob weitere Prüfungshandlungen vorzunehmen sind, um festzustellen, ob die betreffenden Sachverhalte eine Auswirkung auf sein Prüfungsurteil haben.

5.4.3.4. Vollständigkeitserklärung

- 52 Der Prüfer hat vor Abschluss der Prüfung von den gesetzlichen Vertretern eine Vollständigkeitserklärung einzuholen, in der bestätigt wird, dass die Beschreibung des CMS vollständig und richtig ist und dem Prüfer alle relevanten Erklärungen und Nachweise zur Konzeption des CMS sowie zur Angemessenheit, Implementierung und Wirksamkeit des CMS erteilt worden sind. Die Vollständigkeitserklärung ist kein

Ersatz für andere nach diesem *IDW Prüfungsstandard* vorgesehene Prüfungshandlungen.

- 53 Die Vollständigkeitserklärung muss zeitnah zum Datum der Berichterstattung des CMS-Prüfers, aber nicht nach diesem datiert werden.
- 54 Weigern sich die gesetzlichen Vertreter, eine Vollständigkeitserklärung abzugeben, ist darin ein Prüfungshemmnis zu sehen, das dazu führt, dass ein Prüfungsurteil über die CMS-Prüfung nicht erteilt werden kann.

5.4.4. Auswertung der Prüfungsfeststellungen und Ableitung des Prüfungsurteils

- 55 Der Prüfer muss würdigen, ob ausreichende und angemessene Prüfungsnachweise als Grundlage für die Beurteilung der Aussagen der gesetzlichen Vertreter in der CMS-Beschreibung über die Konzeption des CMS (Auftragstyp 1), über die Angemessenheit und Implementierung (Auftragstyp 2) bzw. zur Angemessenheit, Implementierung und Wirksamkeit (Auftragstyp 3) des CMS erlangt wurden. Ist dies der Fall, hat der Prüfer die Prüfungsfeststellungen auszuwerten und ein Prüfungsurteil zu treffen.
- 56 Bestehen keine Beanstandungen, hat der Prüfer ein uneingeschränktes Prüfungsurteil abzugeben. Liegen wesentliche Beanstandungen vor, ist das Prüfungsurteil einzuschränken oder zu versagen. Dies gilt auch für Prüfungshemmnisse, die dazu führen, dass die Aussagen der gesetzlichen Vertreter in der CMS-Beschreibung in wesentlichen Teilen nicht beurteilt werden können.
- 57 Das Prüfungsurteil ist wegen einer Beanstandung einzuschränken, wenn die Beanstandung zwar wesentlich, aber abgrenzbar ist. Sind die Beanstandungen nicht auf bestimmte Teile der Aussagen der gesetzlichen Vertreter in der CMS-Beschreibung abzugrenzen, z.B. weil aufgrund von Mängeln bei der Konzeption des CMS oder einer ungünstigen Compliance-Kultur die Grundsätze und Maßnahmen des CMS insgesamt als nicht angemessen anzusehen sind, ist das Prüfungsurteil zu versagen.
- 58 Liegen Prüfungshemmnisse vor, ist das Prüfungsurteil einzuschränken, wenn die Auswirkungen des Prüfungshemmnisses zwar die Beurteilung eines wesentlichen Teils der Aussagen der gesetzlichen Vertreter in der CMS-Beschreibung ausschließen, eine Beurteilung insgesamt aber noch möglich ist. Kann aufgrund von Prüfungshemmnissen auch nach Ausschöpfung aller prüferischen Möglichkeiten ein Gesamturteil nicht abgegeben werden, ist in der Berichterstattung des CMS-Prüfers darauf hinzuweisen, dass ein Prüfungsurteil nicht erteilt wird.
- 59 Falls sich im Verlauf der Prüfung herausstellt, dass sich die CMS-Beschreibung nicht für eine Prüfung eignet oder sie unangemessene Verallgemeinerungen oder unausgewogene und verzerrende Darstellungen enthält, die eine Irreführung der Berichtsadressaten zur Folge haben können, ist das Prüfungsurteil zu versagen. Dies gilt auch, wenn die angewandten CMS-Grundsätze nicht geeignet sind, um ein angemessenes CMS in den abgegrenzten Teilbereichen einzurichten.

60 Einschränkungen des Prüfungsurteils sind klar durch die Verwendung des Begriffs „Einschränkung“ zu kennzeichnen und zu begründen.

5.5. Dokumentation

61 Der CMS-Prüfer hat die zur Stützung seines Prüfungsurteils dienenden Prüfungsnachweise in den Arbeitspapieren zu dokumentieren. Durch die Arbeitspapiere wird gleichzeitig nachgewiesen, dass die CMS-Prüfung in Übereinstimmung mit diesem *IDW Prüfungsstandard* geplant und durchgeführt wurde. Die Auftragsdokumentation ist innerhalb eines angemessenen Zeitraums nach dem Datum des CMS-Prüfungsberichts abzuschließen.

62 Die Dokumentation muss u.a. die folgenden Nachweise enthalten:

- Einhaltung der Berufspflichten (insb. zum Grundsatz der Unabhängigkeit einschließlich möglicher Unabhängigkeitsgefährdungen und deren Lösung)
- Prüfungshandlungen zur Risikobeurteilung
- Prüfung der Aussagen der gesetzlichen Vertreter in der CMS-Beschreibung zur Konzeption des CMS
- Aufbau- und Funktionsprüfung des CMS
- festgestellte Regelverstöße, die in diesem Zusammenhang vorgenommenen Prüfungshandlungen und an wen diese zu welchem Zeitpunkt berichtet wurden
- Verwertung der Arbeiten von Spezialisten sowie
- Auswertung der Prüfungsfeststellungen und ggf. Gründe für die Einschränkung oder Versagung des Prüfungsurteils.

63 Form und Inhalt der Dokumentation stehen im pflichtgemäßen Ermessen des Wirtschaftsprüfers. Die Arbeitspapiere sind so anzulegen, dass sich ein in CMS-Prüfungen erfahrener Wirtschaftsprüfer, der nicht mit der Prüfung befasst war, in angemessener Zeit ein Bild über die Prüfungsabwicklung und die Prüfungsfeststellungen verschaffen kann.

5.6. Berichterstattung des CMS-Prüfers

5.6.1. CMS-Prüfungsbericht

64 Der Prüfer hat einen schriftlichen CMS-Prüfungsbericht zu verfassen, der ein Prüfungsurteil über die in der CMS-Beschreibung der gesetzlichen Vertreter getroffenen Aussagen enthält. Wenn nach dem Ermessen des Prüfers bestimmte Prüfungsfeststellungen eine unmittelbare Reaktion des Unternehmens erfordern, ist darüber vorab den gesetzlichen Vertretern zu berichten.

65 Der CMS-Prüfungsbericht muss folgende Bestandteile enthalten:

- a) Überschrift: Angabe, dass es sich um den Bericht eines unabhängigen Wirtschaftsprüfers handelt

- b) Berichtsadressaten
- c) Auftragsstyp
- d) Darstellung der oder Bezugnahme auf die vom Unternehmen angewandten CMS-Grundsätze
- e) Gegenstand, Art und Umfang der Prüfung
- f) Abgrenzung der Verantwortlichkeiten der gesetzlichen Vertreter und des CMS-Prüfers
- g) Aussage, dass die Prüfung in Übereinstimmung mit diesem *IDW Prüfungsstandard* durchgeführt wurde
- h) Feststellungen zum CMS und ggf. Empfehlungen
- i) Falls relevant:
 - Beschreibung von bedeutenden Schwierigkeiten bei der Beurteilung des Prüfungsgegenstands anhand der Kriterien
 - Aussage, dass der Auftrag für einen bestimmten Zweck bzw. Adressatenkreis durchgeführt wurde und deshalb die Verwendung der Ergebnisse für andere Zwecke ausgeschlossen ist
- j) Zusammenfassendes Prüfungsurteil in Abhängigkeit von dem vereinbarten Auftragsstyp:
 - Prüfung der Konzeption des CMS (Auftragsstyp 1): Urteil, ob die Aussagen der gesetzlichen Vertreter in der CMS-Beschreibung zur Konzeption des CMS zutreffend dargestellt sind und die CMS-Beschreibung auf sämtliche der in Tz. 19 genannten Grundelemente eines CMS eingeht
 - Prüfung der Aussagen der gesetzlichen Vertreter zur Angemessenheit und Implementierung abgegrenzter Teilbereiche des CMS (Auftragsstyp 2): Urteil, ob die Aussagen der gesetzlichen Vertreter in der CMS-Beschreibung über die Grundsätze und Maßnahmen des CMS in allen wesentlichen Belangen zutreffend dargestellt sind, dass die dargestellten Grundsätze und Maßnahmen in Übereinstimmung mit den angewandten CMS-Grundsätzen geeignet sind, Risiken für wesentliche Regelverstöße mit hinreichender Sicherheit rechtzeitig zu erkennen und Verstöße zu verhindern und dass die Grundsätze und Maßnahmen zu einem bestimmten Zeitpunkt implementiert sind
 - Prüfung der Aussagen der gesetzlichen Vertreter zur Angemessenheit, Implementierung und Wirksamkeit abgegrenzter Teilbereiche des CMS (Auftragsstyp 3): Urteil, ob die Aussagen der gesetzlichen Vertreter in der CMS-Beschreibung über die Grundsätze und Maßnahmen des CMS in allen wesentlichen Belangen zutreffend dargestellt sind, dass die dargestellten Grundsätze und Maßnahmen in Übereinstimmung mit den angewandten CMS-Grundsätzen geeignet sind, Risiken für wesentliche Regelverstöße mit hinreichender Sicherheit rechtzeitig zu erkennen und Verstöße zu verhindern und

dass die Grundsätze und Maßnahmen zu einem bestimmten Zeitpunkt implementiert sind und während eines bestimmten Zeitraums wirksam waren

- k) Eine Aussage über die inhärenten Grenzen des CMS und zum Risiko, die Feststellungen zum CMS auf die Zukunft zu übertragen
- l) Datum des CMS-Prüfungsberichts: Der CMS-Prüfungsbericht ist auf den Tag der Beendigung der Prüfung zu datieren
- m) Name und Ort des Prüfers.

- 66 Da die Prüfung von CMS keine Vorbehaltsaufgabe i.S.d. § 48 Abs. 1 Satz 1 WPO ist, besteht keine Pflicht zur Führung eines Siegels.
- 67 Die CMS-Beschreibung der gesetzlichen Vertreter ist dem CMS-Prüfungsbericht als Anlage beizufügen. Sind in der Beschreibung auch nicht geprüfte Angaben enthalten, ist dies im CMS-Prüfungsbericht zu verdeutlichen.

5.6.2. Weitere Berichtspflichten

- 68 Der Prüfer muss feststellen, ob weitere Berichtspflichten bestehen, z.B. gegenüber dem Aufsichtsorgan des Unternehmens.
- 69 Die Feststellung von Regelverstößen, die sich nicht auf das Prüfungsurteil auswirken, ist grundsätzlich nicht Gegenstand der CMS-Prüfung i.S.d. *IDW Prüfungsstandards*. Im Zusammenhang mit der CMS-Prüfung kann sich jedoch für den Wirtschaftsprüfer aus der Treuepflicht eine Pflicht zur Information des Auftraggebers ergeben, soweit anlässlich der CMS-Prüfung solche Regelverstöße festgestellt werden. Diese Informationspflicht ist im CMS-Prüfungsbericht oder in sonstiger geeigneter Weise zu erfüllen.⁸

6. Anwendungshinweise und Erläuterungen

Vorbemerkungen [Tz. 1 ff.]

- A1 Dieser *IDW Prüfungsstandard* ist nicht anzuwenden bei Aufträgen zur Durchführung vereinbarter Untersuchungshandlungen (sog. *agreed upon procedures*). Unter Aufträgen zur Durchführung vereinbarter Untersuchungshandlungen sind solche Aufträge zu verstehen, bei der ein Wirtschaftsprüfer Untersuchungshandlungen einschließlich einer Berichterstattung hierüber nach zuvor mit dem Auftraggeber vereinbarten Anforderungen durchführt (z.B. ob bei der Erfassung der Reisekosten für eine oder mehrere Personen Belege vorliegen). Dabei wird weder ein zusammengefasstes Gesamturteil über den Untersuchungsgegenstand abgegeben, noch enthält die Berichterstattung einzelne Urteile in Bezug auf die jeweiligen Untersuchungshandlungen. Der Wirtschaftsprüfer berichtet lediglich über seine tatsächlichen Fest-

⁸ Für den Fall, dass der CMS-Prüfer auch Abschlussprüfer des Unternehmens ist, vgl. *IDW Prüfungsstandard: Grundsätze ordnungsmäßiger Berichterstattung bei Abschlussprüfungen (IDW PS 450)* (Stand: 09.09.2009), Tz. 48 ff.

stellungen (*factual findings*) zu den jeweils untersuchten Sachverhalten. Die Schlussfolgerungen sind durch den Berichtsempfänger aus den Feststellungen des Wirtschaftsprüfers zu ziehen.⁹

A2 Folgende abgegrenzte Bereiche können Gegenstand einer CMS-Prüfung sein (ausgewählte Beispiele) (vgl. Tz. 1):

- Rechtsgebiete:
 - Wettbewerbs- und Kartellrecht
 - Antikorruptionsrecht (z.B. § 299 StGB oder Foreign Corrupt Practices Act – FCPA)
 - Börsenrecht (z.B. Vorschriften zum Insiderhandel oder zu Ad-hoc-Meldepflichten)
 - Vorschriften zur Unternehmensführung und -überwachung (z.B. nach dem Deutschen Corporate Governance Kodex)
 - Geldwäschegesetz
 - Verrechnungspreisrecht
 - Umweltrecht
 - Außenwirtschaftsrecht und Exportkontrolle
 - Außensteuerrecht
 - Datenschutz- und Datensicherheitsvorschriften
 - Gleichstellungsverordnung
 - Zollrecht
 - Patentrecht
 - Produkthaftungsrecht
- Geschäftsbereiche bzw. operative Prozesse:
 - Ausschreibung und Vergabe (Einkauf)
 - Provisionszahlungen (Vertrieb)
 - Arbeitssicherheit und technische Sicherheit (Produktion).

Darüber hinaus kommt zusätzlich eine regionale Abgrenzung in Frage, z.B. nach Ländern. Die Abgrenzung von Teilbereichen liegt in der Verantwortung der gesetzlichen Vertreter und ist u.a. abhängig von den rechtlichen und wirtschaftlichen Rahmenbedingungen und der Organisationsstruktur des Unternehmens.

Begriffsbestimmungen [Tz. 5 ff.]

A3 Bei den Grundsätzen und Maßnahmen des CMS (Tz. 6) kann unterschieden werden zwischen Grundsätzen und Maßnahmen, die sich auf das CMS insgesamt bezie-

⁹ Vgl. International Standard on Related Services (ISRS) 4400 „Engagements to perform Agreed-upon Procedures regarding Financial Information“, IFAC, Handbook of International Standards on Auditing, Assurance, and Ethics Pronouncements, New York 2008, Part I, S. 952 ff.

hen, d.h. auf alle von der Unternehmensleitung bestimmten Teilbereiche (z.B. Einrichtung eines Hinweisgeberverfahrens), und solchen Grundsätzen und Maßnahmen, die ausschließlich bestimmte abgegrenzte Teilbereiche betreffen (z.B. eine Genehmigungskontrolle im Einkaufsbereich).

- A4 Allgemein anerkannte Rahmenkonzepte i.S.d. Tz. 9 werden i.d.R. im Rahmen eines transparenten Verfahrens entwickelt, das die Veröffentlichung als Entwurf mit Möglichkeit der Kommentierung durch Fachkreise und interessierte Öffentlichkeit beinhaltet. Die in der Anlage 1 nicht abschließend aufgeführten Rahmenkonzepte genügen diesen Anforderungen.

Gegenstand, Ziel und Umfang der Prüfung [Tz. 12 ff.]

- A5 Art und Umfang der gemäß Tz. 13 in der Verantwortung der gesetzlichen Vertreter liegenden Dokumentation des CMS sind abhängig von den Zielen und der Ausgestaltung des CMS, dem rechtlichen und wirtschaftlichen Umfeld des Unternehmens und den mit der Dokumentation im Einzelnen verfolgten Zielen (z.B. Dokumentation zum Nachweis der Einhaltung von Regeln gegenüber Aufsichtsbehörden).
- A6 Bei der Beurteilung, ob ein angemessen dokumentiertes CMS vorliegt (vgl. Tz. 13) ist zu berücksichtigen, dass eine fehlende oder unvollständige Dokumentation des CMS zu Zweifeln an der dauerhaften Funktionsfähigkeit der eingerichteten Grundsätze und Maßnahmen führen kann. Zum Nachweis der kontinuierlichen Anwendung der Grundsätze und Maßnahmen sollten auch die laufenden Unterlagen über die Festlegung von Compliance-Risiken, deren Analyse und Kommunikation, die Einführung und Kommunikation des Compliance-Programms sowie die Maßnahmen zur Überwachung und Verbesserung des Systems unbeschadet anderer Aufbewahrungspflichten über einen ausreichend langen Zeitraum archiviert werden.
- A7 In der nachfolgenden Tabelle sind die Grundelemente eines CMS und deren Bedeutung im Rahmen der unterschiedlichen Auftragsstypen für CMS-Prüfungen dargestellt (vgl. Tz. 14):

	Auftragstyp 1: Prüfung der Konzeption des CMS	Auftragstyp 2: Prüfung von Angemessenheit und Implementierung des CMS	Auftragstyp 3: Prüfung von Angemessenheit, Implementierung und Wirksamkeit des CMS
Compliance-Kultur	x	x	x
Compliance-Ziele	x	x	x
Compliance-Organisation	x	x	x
Compliance-Risiken	x	x	x

	Auftragstyp 1: Prüfung der Konzeption des CMS	Auftragstyp 2: Prüfung von Angemessenheit und Implementierung des CMS	Auftragstyp 3: Prüfung von Angemessenheit, Implementierung und Wirksamkeit des CMS
Compliance-Programm			
Prozess der Erstellung des Programms	x	x	x
Eignung der Grundsätze und Maßnahmen		x	x
Wirksamkeit der Grundsätze und Maßnahmen			x
Compliance-Kommunikation			
Entwicklung des Kommunikationsprozesses	x	x	x
Eignung der Kommunikationsmaßnahmen		x	x
Wirksamkeit der Kommunikationsmaßnahmen			x
Compliance-Überwachung und Verbesserung			
Entwicklung von Verfahren zur Überwachung und Verbesserung des CMS	x	x	x
Eignung der Überwachungs- und Verbesserungsmaßnahmen		x	x
Wirksamkeit der Überwachungs- und Verbesserungsmaßnahmen			x

- A8 *Hinreichende Sicherheit* bedeutet nicht absolute Sicherheit: Auch ein ansonsten wirksam erscheinendes CMS unterliegt systemimmanenten Grenzen, sodass möglicherweise auch wesentliche Regelverstöße auftreten können, ohne systemseitig verhindert oder aufgedeckt zu werden. Diese systemimmanenten Grenzen ergeben sich u.a. aus menschlichen Fehlleistungen (bspw. infolge von Nachlässigkeit, Ablenkungen, Beurteilungsfehlern und Missverstehen von Arbeitsanweisungen), Missbrauch oder Vernachlässigung der Verantwortung durch für bestimmte Maßnahmen verantwortliche Personen, der Umgehung oder Außerkraftsetzung von Kontrollen durch Zusammenarbeit zweier oder mehrerer Personen oder dem Verzicht des Managements auf bestimmte Maßnahmen, weil die Kosten dafür höher eingeschätzt werden als der erwartete Nutzen.
- A9 Gemäß Tz. 17 ist die Wirksamkeit des CMS dann gegeben, wenn die Grundsätze und Maßnahmen von den hiervon Betroffenen nach Maßgabe ihrer Verantwortung zur Kenntnis genommen und bei der täglichen Arbeit beachtet werden. Der Kreis der „Betroffenen“ hängt jeweils von den zu beachtenden Regeln ab und muss nicht auf die vom Unternehmen beschäftigten Mitarbeiter begrenzt sein. Zum Beispiel kommen auch Mitarbeiter eines Zulieferers des Unternehmens als von den Grundsätzen und Maßnahmen Betroffene in Betracht, wenn dies mit dem Zulieferer vereinbart wurde.

Grundelemente eines CMS [Tz. 19]

Compliance-Kultur

- A10 Die Angemessenheit und Wirksamkeit des CMS wird wesentlich durch die Compliance-Kultur im zu prüfenden Unternehmen geprägt. Merkmale sind z.B.
- die Integrität der gesetzlichen Vertreter,
 - das Bekenntnis des Managements zur Bedeutung eines verantwortungsvollen Verhaltens im Einklang mit den zu beachtenden Regeln,
 - die von den gesetzlichen Vertretern aufgestellten und kommunizierten Verhaltensgrundsätze,
 - die Anreizsysteme, mit denen regelkonformes Verhalten gefördert wird, einschließlich der Berücksichtigung von Compliance bei Personalbeurteilungen und Beförderungen,
 - der Führungsstil und die Personalpolitik des Unternehmens (z.B. Bedeutung der Kompetenz und Erfahrung der Mitarbeiter) sowie
 - die Stellung des und die Art der Aufgabenwahrnehmung durch das Aufsichtsorgan im Zusammenhang mit Risikomanagement und Compliance.

Bei einer günstigen Compliance-Kultur, bei der die Beachtung der relevanten Anforderungen eine hohe Bedeutung hat und aufgedeckte Verstöße angemessene Sanktionen nach sich ziehen, werden die im CMS verankerten Regelungen von den Mitarbeitern eher beachtet als bei einer ungünstigen Compliance-Kultur.

Compliance-Organisation

A11 Merkmale einer Compliance-Organisation sind u.a.

- die klare Festlegung von Rollen und Verantwortlichkeiten im CMS, z.B. die Bestimmung eines Compliance-Beauftragten¹⁰ bzw. eines Compliance-Gremiums einschließlich der Festlegung der Aufgaben und der hierarchischen Stellung bzw. der organisatorischen Einordnung sowie der Berichtslinien,
- die Bereitstellung von im Hinblick auf die Compliance-Ziele und Compliance-Risiken ausreichenden Ressourcen zur Konzeption, Einführung, Durchsetzung und Überwachung sowie kontinuierlichen Verbesserung des CMS,
- die Integration des CMS in andere bestehende Systeme der Unternehmensorganisation, wie z.B. das Risikomanagementsystem oder das interne Kontrollsystem, und
- die Entwicklung organisatorischer und technischer Hilfsmittel zu den einzelnen CMS-Bestandteilen, insb. zum Compliance-Programm, zur Compliance-Kommunikation und zur Überwachung des CMS. Hierbei kann es sich z.B. um Handbücher, manuelle Checklisten oder IT-Tools handeln.

Compliance-Ziele

A12 Die Festlegung der Compliance-Ziele erfolgt in Übereinstimmung mit den allgemeinen Unternehmenszielen und umfasst insb. die Abgrenzung der Teilbereiche und der in den Teilbereichen zu beachtenden Regeln. Hierbei wird auch der Sicherheitsgrad festgelegt, mit dem das CMS Regelverstöße verhindern soll. Bei der Festlegung der Compliance-Ziele sollten u.a. die folgenden Anforderungen beachtet werden:

- Konsistenz der unterschiedlichen Ziele
- Verständlichkeit und Praktikabilität der Ziele
- Messbarkeit des Grades der Zielerreichung und
- Abstimmung mit den verfügbaren Ressourcen.

Compliance-Risiken

A13 Die Feststellung und Beurteilung von Compliance-Risiken stellt die Grundlage für die Entwicklung eines angemessenen Compliance-Programms dar. Das Unternehmen führt zu diesem Zweck für die abgegrenzten Teilbereiche des CMS eine systematische Aufnahme der Risiken für Regelverstöße durch, z.B. in Form von Interviews, Workshops oder der Auswertung von verfügbaren Informationen anderer Unternehmen. Bei der Risikoanalyse werden die grundsätzlichen Entscheidungen der

¹⁰ Für Compliance-Beauftragte können sich ggf. aufgrund ihrer besonderen Aufgabengebiete und einer daraus folgenden möglichen Garantenpflicht besondere Haftungsrisiken ergeben (vgl. BGH-Urteil (Az 5 StR 394/08) vom 17.07.2009).

gesetzlichen Vertreter zur Risikosteuerung (Risikovermeidung, Risikoreduktion, Risikoüberwälzung oder Risikoakzeptanz) berücksichtigt.

Allgemeine Faktoren, die für die Risikoanalyse relevant sein können, sind u.a.

- Änderungen im wirtschaftlichen und rechtlichen Umfeld,
- Personalveränderungen,
- überdurchschnittliches Unternehmenswachstum,
- neue Technologien,
- neue oder atypische Geschäftsfelder oder Produkte,
- Umstrukturierungen und
- Expansion in neue Märkte.

Die Befassung mit den Compliance-Risiken ist keine einmalige Aktivität, sondern ein Regelprozess, der einen wesentlichen Bestandteil der kontinuierlichen Weiterentwicklung und Verbesserung des CMS darstellt.

Compliance-Programm

- A14 Ein Compliance-Programm setzt sich aus den Grundsätzen und Maßnahmen zusammen, die auf die Begrenzung der Compliance-Risiken und damit auf ein regelkonformes Verhalten abzielen.

Bei den Grundsätzen handelt es sich um Regelungen, mit denen die Mitarbeiter und ggf. Dritte zu regelkonformem Verhalten angehalten werden. Sie enthalten klare Festlegungen zur Zulässigkeit bzw. Unzulässigkeit bestimmter Aktivitäten sowie zu den Maßnahmen des Compliance-Programms, die zur Sicherstellung der Compliance zu beachten sind.

Die Maßnahmen des Compliance-Programms zielen auf die Verhinderung von Regelverstößen ab (Prävention); dies umfasst auch das rechtzeitige Erkennen von Risiken für Compliance-Verstöße (z.B. durch die Einrichtung eines Hinweisgeberverfahrens) und die Reaktionen auf die erkannten Risiken. Für den Fall der Aufdeckung von Verstößen stellen die Maßnahmen eine Kommunikation an die zuständigen Stellen im Unternehmen und erforderlichenfalls an die zuständigen externen Stellen (z.B. bei Verdacht auf Verstöße gegen das Geldwäschegesetz) sowie eine Analyse der Ursachen für die Verstöße sicher. Eine solche Ursachenanalyse stellt eine Grundlage für die Verbesserung des CMS dar.

Zu den Maßnahmen des Compliance-Programms zählen weiterhin die in das CMS integrierten Kontrollen, mit denen die Einhaltung der Grundsätze und die Durchführung der Maßnahmen sichergestellt werden. Hierbei handelt es z.B. um

- Funktionstrennungen,
- Berechtigungskonzepte,
- Genehmigungsverfahren und Unterschriftenregelungen,
- Vorkehrungen zum Vermögensschutz und andere Sicherheitskontrollen,

- unabhängige Gegenkontrollen (4-Augen-Prinzip) und
- Job-Rotationen.

Konkrete Beispiele für die Bestandteile von Compliance-Programmen sind in den in der Anlage 1 dargestellten CMS-Rahmenkonzepten enthalten.

Compliance-Kommunikation

A15 Die Compliance-Kommunikation umfasst u.a. die folgenden Elemente:

- Kommunikation der in den Teilbereichen zu beachtenden Regeln sowie des Compliance-Programms an die betroffenen Personen
- Festlegung der Berichtspflichten (Anlässe) und der Berichtswege für die Kommunikation von Compliance-Risiken und festgestellten bzw. vermuteten Regelverstößen an die zuständigen Stellen im Unternehmen
- Kommunikation der Ergebnisse von Überwachungsmaßnahmen zwecks Ursachenanalyse und Entwicklung von Maßnahmen zur Verbesserung des CMS.

Die Compliance-Kommunikation kann z.B. in Form von Mitarbeiterbriefen, Compliance-Handbüchern oder Schulungsveranstaltungen erfolgen.

Voraussetzung für eine wirksame Compliance-Kommunikation sind ausreichende Kenntnisse über die Berichtspflichten und ein Bewusstsein der Mitarbeiter bzw. der betroffenen Dritten für die Bedeutung einer zeitnahen und vollständigen Kommunikation.

Compliance-Überwachung und Verbesserung

A16 Bei der Compliance-Überwachung handelt es sich um Überwachungsmaßnahmen durch prozessunabhängige Stellen, z.B. die Interne Revision. Die Compliance-Überwachung zielt darauf ab, festzustellen, ob das CMS unter Beachtung der angewandten CMS-Grundsätze angemessen ausgestaltet und wirksam ist. Dies beinhaltet auch, ob die prozessintegrierten Kontrollen (vgl. Tz. A14) wirksam sind. Zur Compliance-Überwachung zählen u.a. folgende Aspekte:

- Festlegung der Zuständigkeiten für die Compliance-Überwachung
- Entwicklung eines Überwachungsplans
- Bereitstellung von ausreichend erfahrenen Ressourcen für die Durchführung der Überwachungsmaßnahmen
- Bestimmung der Berichtswege für die Ergebnisse der Überwachungsmaßnahmen sowie
- Erstellung von Berichten über die Ergebnisse der Überwachungsmaßnahmen und Auswertung der Berichte durch die zuständige Stelle.

Die Ergebnisse der Überwachungsmaßnahmen werden daraufhin untersucht, ob es Hinweise auf Schwachstellen im CMS gibt. Im Falle solcher Hinweise werden Maßnahmen zur Erhöhung der Wirksamkeit des CMS entwickelt, z.B. eine intensivere

Kommunikation des Compliance-Programms oder die Einführung zusätzlicher Kontrollen.

Ergeben sich im Rahmen der Überwachung oder bei sonstigen Maßnahmen des CMS Hinweise auf Regelverstöße von Mitarbeitern oder Dritten, sollten als Bestandteil der Durchsetzung des CMS erkennbare Maßnahmen getroffen werden, um solche Vorfälle in der Zukunft zu vermeiden. Hierbei kann es sich z.B. um zusätzliche Schulungsmaßnahmen oder die Berücksichtigung dieser Informationen bei der Mitarbeiterbeurteilung und bei der Entscheidung über Beförderungen handeln. Bei gravierenden Verstößen bzw. bei Missachtung wesentlicher Grundsätze oder Maßnahmen des CMS kann auch die Kündigung des Arbeitsvertrags oder die Kündigung von Verträgen mit Dritten in Betracht kommen.

Das Aufsichtsorgan sollte über die Maßnahmen zur Überwachung und Verbesserung des CMS informiert werden, soweit es der Erfüllung der eigenen Überwachungsfunktion des Aufsichtsorgans dient (z.B. § 107 Abs. 3 AktG).¹¹

Auftragsannahme [Tz. 21 ff.]

A17 Folgende Fragen haben bei der Beurteilung der Eignung des in der CMS-Beschreibung dargestellten Systems als Prüfungsgegenstand eine besondere Bedeutung (vgl. Tz. 23):

- Übernehmen die gesetzlichen Vertreter Verantwortung für Einrichtung, Aufrechterhaltung, Überwachung und Durchsetzung des CMS?
- Ist das CMS (Auftragstyp 2 und 3) bzw. die Konzeption des CMS (Auftragstyp 1) in einer Weise dokumentiert, dass ein sachverständiger Dritter in angemessener Zeit einen Überblick über das CMS bzw. die Konzeption des CMS erhalten kann?
- Sind die zu prüfenden Teilbereiche des CMS klar abgegrenzt?
- Hat das Unternehmen bei der Konzeption des CMS ein strukturiertes Vorgehen gewählt und geeignete CMS-Grundsätze verwendet, die vom Prüfer als Prüfungskriterien zugrunde gelegt werden können (vgl. Tz. 8 f. und Anlage 1)?

A18 Folgende Aspekte werden im Allgemeinen mit dem Auftraggeber schriftlich vereinbart (vgl. Tz. 25):

- Ziel und Gegenstand der CMS-Prüfung (vgl. Tz. 12 ff.)
- die Verantwortung der gesetzlichen Vertreter für das CMS sowie deren Bereitschaft, eine CMS-Beschreibung zu erstellen
- die vom Unternehmen angewandten CMS-Grundsätze
- Art und Umfang der Prüfung des CMS und der Berichterstattung einschließlich einer Bezugnahme auf diesen *IDW Prüfungsstandard*
- die Tatsache, dass die Prüfung der Aussagen der gesetzlichen Vertreter zum CMS risikoorientiert erfolgt und keine Vollprüfung, sondern eine Prüfung in Stich-

¹¹ Vgl. Deutscher Corporate Governance Kodex (DCGK) Ziff. 5.3.2.

proben vorgenommen wird und deshalb ein unvermeidbares Risiko besteht, dass selbst wesentliche falsche Aussagen der gesetzlichen Vertreter in der CMS-Beschreibung bzw. wesentliche Mängel im CMS unentdeckt bleiben

- ein Hinweis darauf, dass ein CMS nicht jeden Verstoß vermeiden kann und die Prüfung nicht darauf ausgerichtet ist, einzelne Verstöße aufzudecken
- bei Auftragsstyp 3: Zeitraum, auf den sich die Funktionsprüfung des CMS beziehen soll
- Hinweise auf die Verwertung von Arbeiten der internen Revision sowie von Spezialisten
- das Erfordernis eines unbeschränkten Zugangs des Prüfers zu den für die Prüfung erforderlichen Informationen und der Bereitschaft der gesetzlichen Vertreter, Auskünfte in dem erforderlichen Umfang vollständig und richtig zu erteilen
- die Grundlagen der Honorarabrechnung und den Auslagenersatz
- Haftungsbeschränkungen
- die Verpflichtung der gesetzlichen Vertreter, eine Vollständigkeitserklärung abzugeben
- ggf. Verwendungsvorbehalt der Berichterstattung sowie
- ggf. Hinweis auf Berichtspflichten gegenüber dem Aufsichtsorgan.

A19 Wenn der CMS-Prüfer auch mit anderen Dienstleistungen (z.B. der Jahresabschlussprüfung) beauftragt war und er in deren Rahmen für die Beurteilung der Aussagen der gesetzlichen Vertreter zum CMS relevante Informationen erlangt hat, sollte er vereinbaren, dass er das Ergebnis dieser Tätigkeiten bei der Prüfung des CMS berücksichtigen wird.

Wesentlichkeit [Tz. 33 f.]

A20 Der Prüfer berücksichtigt seine Überlegungen zur Wesentlichkeit (vgl. Tz. 33)

- bei der Planung von Art, Umfang und Zeitpunkt der Prüfungshandlungen,
- bei der Auswertung von Prüfungsfeststellungen, d.h. bei der Beurteilung, ob die Aussagen der gesetzlichen Vertreter über das CMS wesentliche Fehler enthalten, und
- bei der Würdigung von anlässlich der CMS-Prüfung festgestellten Verstößen.

A21 Ein wesentlicher Fehler in den Aussagen der gesetzlichen Vertreter in der CMS-Beschreibung kann z.B. dann vorliegen, wenn

- sie einen vorhandenen wesentlichen Mangel des CMS nicht erkennen lassen,
- sie falsche Angaben enthalten, die für den Berichtsadressaten entscheidungsrelevant sein können, oder
- sie unangemessene Verallgemeinerungen oder unausgewogene und verzerrende Darstellungen enthalten, die eine Irreführung der Berichtsadressaten zur Folge haben können.

- A22 Ein wesentlicher Mangel des CMS liegt dann vor, wenn das CMS Risiken für wesentliche Verstöße gegen die Regeln, auf deren Einhaltung das CMS in den vom Unternehmen abgegrenzten Teilbereichen ausgerichtet ist, nicht mit hinreichender Sicherheit rechtzeitig erkennt und Verstöße verhindert. Ein wesentlicher Mangel des CMS kann auch bei einer Kumulation von nicht rechtzeitig erkannten Risiken und nicht vom System verhinderten Verstößen vorliegen, die einzeln betrachtet nicht wesentlich sind.
- A23 Bei der Bestimmung der Wesentlichkeit von (möglichen) Verstößen sind insb. folgende Fragestellungen von Bedeutung (vgl. Tz. 34):
- *Bedeutung der verletzten Regel:* Handelt es sich um eine kriminelle Handlung oder eine Ordnungswidrigkeit oder hat der Verstoß keine rechtliche Relevanz? Handelt es sich um einen Verstoß gegen Regelungen, die der Einhaltung gesetzlicher Vorschriften dienen, oder gegen andere Regelungen?
 - *Folgen des Verstoßes:* Ist mit dem Verstoß ein hoher finanzieller oder sonstiger Schaden für das Unternehmen verbunden?
 - *Motivation für den Verstoß:* Handelt es sich um einen beabsichtigten oder einen unbeabsichtigten Verstoß? Ist mit dem Verstoß eine persönliche Bereicherung oder ein sonstiger Vorteil verbunden?
 - *Tragweite des Verstoßes:* Ist der Verstoß auf eine systemimmanente Schwachstelle zurückzuführen oder handelt es sich um eine einmalige Durchbrechung des Systems? Wurden interne Kontrollen durch Mitglieder des Managements außer Kraft gesetzt?

Prüfungsdurchführung [Tz. 35]

- A24 Risiken für wesentliche Mängel des CMS können sich u.a. aus den folgenden Umständen ergeben:
- Es werden keine angemessenen CMS-Grundsätze verwendet.
 - Die Konzeption des CMS weist Lücken auf, die dazu führen können, dass nicht alle Risiken für wesentliche Verstöße berücksichtigt werden.
 - Die Grundsätze und Maßnahmen des CMS werden nicht regelmäßig auf Anpassungsbedarf wegen geänderter Rahmenbedingungen überprüft und ggf. geändert.
 - Das CMS wird im Unternehmen nicht ausreichend kommuniziert und überwacht.
 - Das CMS wird nicht konsequent durchgesetzt, z.B. wenn bei aufgedeckten Verstößen die Nichtbeachtung des CMS durch die Mitarbeiter keine wirksamen Konsequenzen hat.

Kenntnisse über das rechtliche und wirtschaftliche Umfeld des Unternehmens [Tz. 36]

- A25 Sofern es sich bei dem CMS-Prüfer um den Abschlussprüfer des Unternehmens handelt, werden die erforderlichen Kenntnisse teilweise bereits vorhanden sein.¹² Die Abschlussprüfung hat im Unterschied zur CMS-Prüfung allerdings das Ziel, die Ordnungsmäßigkeit der Rechnungslegung zu beurteilen. Der Abschlussprüfer richtet seine Risikobeurteilungen auf die Feststellung wesentlicher falscher Angaben in der Rechnungslegung aus. Die in diesem Zusammenhang erworbenen Kenntnisse über das rechtliche Umfeld des Unternehmens werden daher für Zwecke der CMS-Prüfung im Allgemeinen nicht ausreichend sein.

Konzeption des CMS (Auftragstypen 1, 2 und 3) [Tz. 37 ff.]

- A26 Im Rahmen der Konzeption des CMS entscheiden die gesetzlichen Vertreter, welche CMS-Grundsätze angewendet werden sollen. Hierbei kommen die in Anlage 1 genannten allgemein anerkannten Rahmenkonzepte, andere angemessene Rahmenkonzepte oder individuell entwickelte angemessene CMS-Grundsätze in Betracht. Bei der individuellen Entwicklung von CMS-Grundsätzen können die gesetzlichen Vertreter auch entscheiden, sich bei der Ausgestaltung des CMS an verfügbaren Informationen über die Praxis anderer Unternehmen zu orientieren. Sofern das angewandte Rahmenkonzept nicht alle CMS-Grundelemente (vgl. Tz. 19) abdeckt, bietet sich eine Ergänzung durch andere Grundsätze an, die individuell entwickelt, im Rahmen von Vergleichen mit der Praxis anderer Unternehmen festgestellt oder einem anderen Rahmenkonzept entnommen werden können.
- A27 Als Prüfungshandlungen zur Beurteilung der beschriebenen Konzeption des CMS (vgl. Tz. 39) kommen insb. Befragungen des Managements und anderer Personen und die Durchsicht von Organisationsunterlagen, wie Protokolle und Sitzungsberichte, Berichte der internen Revision, Handbücher und Verfahrensgrundsätze in Betracht.

Aufbau- und Funktionsprüfung des CMS (Auftragstypen 2 und 3) [Tz. 40 ff.]

- A28 Bei der Festlegung der Prüfungshandlungen kann der Prüfer bei wiederkehrenden Aufträgen Ergebnisse früherer CMS-Prüfungen verwerten. Dies gilt vor allem für die Beurteilung des Aufbaus des CMS, die sich bei Folgeprüfungen vor allem auf Veränderungen des CMS erstrecken wird. Zur Beurteilung der Wirksamkeit des CMS im Prüfungszeitraum wirken sich die Erkenntnisse aus früheren Prüfungen im Wesentlichen auf die Risikoeinschätzung des CMS-Prüfers und den Umfang der Funktions-

¹² Vgl. *IDW Prüfungsstandard: Feststellung und Beurteilung von Fehlerrisiken und Reaktionen des Abschlussprüfers auf die beurteilten Fehlerrisiken (IDW PS 261)* (Stand: 09.09.2009) und *IDW Prüfungsstandard: Kenntnisse über die Geschäftstätigkeit sowie das wirtschaftliche und rechtliche Umfeld des zu prüfenden Unternehmens im Rahmen der Abschlussprüfung (IDW PS 230)* (Stand: 08.12.2005).

prüfungen aus. Prüfungsnachweise aus früheren Prüfungen stellen aber für sich genommen keinen Nachweis zur Wirksamkeit des CMS im zu prüfenden Zeitraum dar.

- A29 Im Rahmen der Aufbauprüfung (vgl. Tz. 41) kommen in Bezug auf die zu prüfenden Teilbereiche insb. folgende Prüfungshandlungen in Betracht:
- Befragungen von Mitgliedern des Managements und von Mitgliedern des Aufsichtsorgans (z.B. zur Konzeption des CMS, zur Durchsetzung des CMS, zu bekannten Schwachstellen im CMS sowie zu festgestellten Regelverstößen)
 - Befragungen von Personen, die für die Überwachung des CMS und die Koordination von Aktivitäten im Zusammenhang mit dem CMS zuständig sind, um deren Aufgabenstellung, Kompetenz und Erfahrung, Stellung innerhalb der Unternehmenshierarchie und Kenntnisse über mögliche Schwachstellen im CMS und festgestellte Verstöße gegen zu beachtende Regeln oder gegen im Compliance-Programm verankerte Grundsätze und Maßnahmen sowie die Reaktionen des Unternehmens auf solche Feststellungen in Erfahrung zu bringen (z.B. Interne Revision und Compliance-Beauftragter)
 - Durchsicht von Dokumentationen des CMS (z.B. Organisationshandbücher, in denen Verantwortlichkeiten und Maßnahmen zur Sicherstellung der Compliance geregelt sind, sowie entsprechende Anweisungen an die Mitarbeiter)
 - Durchsicht von Unterlagen, die durch das CMS generiert werden (z.B. Dokumentation zu festgestellten Verstößen und Sanktionen bei festgestellten Verstößen)
 - Beobachtung von Aktivitäten und Arbeitsabläufen im Unternehmen, die mit dem CMS in Verbindung stehen.
- A30 Die Funktionsprüfung (vgl. Tz. 42) betrifft die Anwendung der im CMS verankerten Grundsätze und Maßnahmen, die Kontinuität der Anwendung und die Frage, ob das Compliance-Programm wie vorgesehen von den dafür bestimmten Personen durchgeführt wurde und diesen die für die Wahrnehmung der Aufgaben erforderlichen Informationen zur Verfügung standen.
- A31 Art, Umfang und Zeitpunkt der im Rahmen der Aufbau- und Funktionsprüfung (vgl. Tz. 41) durchzuführenden Prüfungshandlungen sind u.a. abhängig von
- den von den gesetzlichen Vertretern gewählten CMS-Grundsätzen,
 - den Inhalten der CMS-Beschreibung der gesetzlichen Vertreter,
 - den bisherigen Erfahrungen des Prüfers mit dem Unternehmen,
 - den Ergebnissen der Risikobeurteilungen,
 - der Ausgestaltung des CMS und dessen Dokumentation,
 - der Art und Weise der Überwachung des CMS, z.B. durch die Interne Revision sowie
 - Wesentlichkeitsüberlegungen.
- A32 Folgende Prüfungshandlungen kommen im Rahmen der Funktionsprüfung des CMS insb. in Betracht (vgl. Tz. 42 f.):

- Befragung von Mitarbeitern
- Durchsicht von Nachweisen über die Einhaltung des Compliance-Programms, z.B. Kommunikation eines Verhaltenskodex, Trainingsdokumentation, schriftliche Erklärungen der Mitarbeiter oder Meldungen im Beschwerdemanagement
- Beobachtung der Durchführung von in der CMS-Beschreibung dargestellten Maßnahmen
- Nachvollzug von Kontrollaktivitäten
- Einsichtnahme in Berichte der Internen Revision oder des Compliance-Beauftragten an die gesetzlichen Vertreter bzw. das Aufsichtsorgan.

Verwertung der Arbeit von Spezialisten [Tz. 46 ff.]

- A33 Eine Verwertung der Arbeit von Spezialisten (vgl. Tz. 46) kann z.B. geboten sein bei
- der Frage der Angemessenheit des CMS, um die Beachtung spezieller Rechtsvorschriften zu gewährleisten,
 - der Interpretation spezifischer Anforderungen der angewandten CMS-Grundsätze,
 - der Beurteilung von IT-gestützten Bestandteilen des CMS sowie
 - der Würdigung von Sachverhalten, die auf einen Verstoß hindeuten, und der Würdigung von festgestellten Verstößen.
- A34 Die Beurteilung der Arbeit von Spezialisten (vgl. Tz. 49) kann z.B. im Rahmen von Befragungen oder der Durchsicht der Berichterstattung bzw. der Arbeitspapiere des externen Spezialisten erfolgen.

Ereignisse bis zum Datum der Berichterstattung über die CMS-Prüfung [Tz. 50 f.]

- A35 Als Prüfungshandlungen zur Feststellung von Ereignissen nach dem in der CMS-Beschreibung genannten Zeitpunkt/Zeitraum, auf den sich die Aussagen der gesetzlichen Vertreter beziehen (vgl. Tz. 50), kommen z.B. in Betracht:
- kritisches Lesen von Protokollen über in diesem Zeitraum stattgefundene Sitzungen der Verwaltungsorgane
 - kritisches Lesen von unternehmensinternen Berichten, wie z.B. Berichte des Compliance-Beauftragten oder der internen Revision an die Unternehmensleitung, sowie
 - Befragungen des Compliance-Beauftragten und erforderlichenfalls der gesetzlichen Vertreter und des Aufsichtsorgans. Die Befragungen können sich bspw. auf bis zum Zeitpunkt der Berichterstattung über die CMS-Prüfung aufgedeckte oder vermutete Verstöße beziehen, die die Angemessenheit und Wirksamkeit des CMS in Frage stellen.

Anlagen

1. Allgemein anerkannte CMS-Rahmenkonzepte

Name	Organisation	Anwendungsbereich
1. Allgemeine Rahmenkonzepte		
Foundation Guidelines "Red Book" ¹³	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.
Australian Standard on Compliance Programs (AS 3806-2006) ¹⁴	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) ¹⁵	Committee of Sponsoring Organization, Jersey City, USA	Umfassendes Modell eines unternehmensweiten Risikomanagements
OECD Grundsätze der Corporate Governance ¹⁶	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD), Phoenix, USA	Grundsätze der OECD für Corporate Governance, die weltweit Mindeststandards setzen sollen

¹³ <http://www.oceg.org/standards>.

¹⁴ <http://www.saiglobal.com/PDFTemp/Previews/OSH/as/as3000/3800/3806-2006.pdf>.

¹⁵ <http://www.coso.org/default.htm>.

¹⁶ <http://www.oecd.org/dataoecd/57/19/32159487.pdf>.

Name	Organisation	Anwendungsbereich
OECD Guidelines for Multi-national Enterprises ¹⁷	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD), Phoenix, USA	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 ¹⁸	Initiative Corporate Governance der deutschen Immobilienwirtschaft e.V., Berlin	Grundsätze für eine transparente und professionelle Unternehmensführung in der Immobilienwirtschaft
Grundsätze ordnungsmäßiger Compliance ¹⁹	Österreichische Finanzmarktaufsicht, Wien, Österreich	Grundsätze ordnungsmäßiger Compliance für österreichische Kreditinstitute, die Geschäfte und Dienstleistungen im Zusammenhang mit Finanzinstrumenten durchführen
United States Federal Sentencing Guidelines ²⁰	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 ²¹	Partnering Against Corruption Initiative (PACI), Genf, Schweiz	Prinzipien zur Verhinderung von Bestechung
OFT Guide for Compliance with Competition Law ²²	Office of fair trading (OFT), London, England (<i>non-ministerial government department</i> in UK)	Grundsätze zur Einhaltung von Vorschriften des Wettbewerbsrechts

¹⁷ <http://www.oecd.org/dataoecd/56/36/1922428.pdf>.

¹⁸ <http://www.immo-initiative.de/>.

¹⁹ <http://www.fma.gv.at/cms/site/DE/detail.html?doc=CMS1200476216866&channel=CH0388>.

²⁰ <http://www.ussc.gov/2009guid/GL2009.pdf>.

²¹ http://www.gopacnetwork.org/Docs/Main/PACI_Principles_EN.pdf.

²² http://www.oft.gov.uk/shared_of/business_leaflets/ca98_mini_guides/oft424.pdf.

Name	Organisation	Anwendungsbereich
Korruption bekämpfen – Ein ICC-Verhaltenskodex für die Wirtschaft ²³	ICC Deutschland e.V., Internationale Handelskammer, Berlin / Deutscher Industrie- und Handelskammertag e.V., Berlin	Verhaltenskodex zur Korruptionsbekämpfung
Geschäftsgrundsätze für die Bekämpfung von Korruption ²⁴	Transparency International Deutschland e.V., Berlin	Geschäftsgrundsätze für die Bekämpfung von Korruption
BME-Verhaltensrichtlinie Code of Conduct ²⁵	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.

2. Berichterstattung über CMS-Prüfungen

Formulierungsbeispiele für Berichterstattungen über CMS-Prüfungen

2.1. Auftragstyp 1

Bericht des unabhängigen Wirtschaftsprüfers

Die Prüfung der Konzeption des Compliance Management Systems für ... [Beschreibung des oder der abgegrenzten Teilbereiche(s)]

An die [Gesellschaft]

A. Prüfungsauftrag

Mit Schreiben vom [Datum] haben uns [die gesetzlichen Vertreter] der [Gesellschaft] beauftragt, eine Prüfung der in nachstehender Anlage 1 beigefügten Beschreibung der Konzeption ihres Compliance Management Systems für ... [Beschreibung des oder der abgegrenzten Teilbereiche(s)] durchzuführen.

Unter einem Compliance Management System (CMS) sind die Grundsätze und Maßnahmen eines Unternehmens zu verstehen, die auf die Sicherstellung eines regelkonformen Verhaltens des Unternehmens und seiner Mitarbeiter sowie ggf. Dritten abzielen, d.h. auf die Ein-

²³ http://www.icc-deutschland.de/fileadmin/ICC_Dokumente/ICC-Verhaltenskodex_Korruption_final.pdf.

²⁴ http://www.transparency.de/fileadmin/pdfs/Themen/Wirtschaft/Business_Principles_German.pdf.

²⁵ http://www.bme.de/fileadmin/pdf/Pressemeldungen/2008_11_10_BME_VerhaltensrichtlinieCoC.pdf.

haltung bestimmter Regeln bzw. die Verhinderung von wesentlichen Verstößen gegen Regeln in abgegrenzten Teilbereichen (Regelverstöße).

Die Konzeption eines CMS umfasst die Förderung einer günstigen Compliance-Kultur sowie den Aufbau der Compliance-Organisation (Aufbau- und Ablauforganisation), die Festlegung der Compliance-Ziele, den Prozess der Feststellung und Analyse der Compliance-Risiken durch das Unternehmen, den Prozess der Erstellung des Compliance-Programms, die Entwicklung des Kommunikationsprozesses sowie von Verfahren zur Überwachung und Verbesserung des CMS.

Für die Durchführung des Auftrags und unsere Verantwortlichkeit sind, auch im Verhältnis zu Dritten, die diesem Bericht beigefügten Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 01.01.2002 vereinbart.

Über Art und Umfang sowie über das Ergebnis unserer Prüfung erstatten wir diesen Bericht, der ausschließlich an die Gesellschaft zur Verwendung für [interne Zwecke] gerichtet ist.

[alternativ: Wir erstellen diese Berichterstattung auf Grundlage des mit der ... [Gesellschaft] geschlossenen Auftrags, dem, auch mit Wirkung gegenüber Dritten, die beiliegenden Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 01.01.2002 mit der Maßgabe zugrunde liegen, dass die darin enthaltenen Haftungshöchstgrenzen allen Personen gegenüber, die diese Berichterstattung mit unserer vorherigen Zustimmung erhalten haben, gemeinschaftlich besteht.]

B. Gegenstand, Art und Umfang der Prüfung

Gegenstand unserer Prüfung waren die in der als Anlage 1 beigefügten CMS-Beschreibung enthaltenen Aussagen der gesetzlichen Vertreter zur Konzeption des CMS für ... [Beschreibung des oder der abgegrenzten Teilbereiche(s)]. Die gesetzlichen Vertreter haben die CMS-Grundsätze [Bezeichnung der CMS-Grundsätze] zugrunde gelegt.

Die Verantwortung für das CMS einschließlich der Dokumentation des CMS und für den Inhalt der CMS-Beschreibung liegt bei den gesetzlichen Vertretern der Gesellschaft.

Unsere Aufgabe ist es, auf Grundlage der von uns durchgeführten Prüfung eine Beurteilung über die in der CMS-Beschreibung enthaltenen Aussagen der gesetzlichen Vertreter zur Konzeption des CMS abzugeben. Die Prüfung ist nicht darauf ausgerichtet, Prüfungssicherheit über die tatsächliche Einhaltung von Regeln zu erlangen.

Wir haben unsere Prüfung auf der Grundlage der für Wirtschaftsprüfer geltenden Berufspflichten unter Beachtung des *IDW Prüfungsstandards: Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen (IDW PS 980)* durchgeführt. Hiernach haben wir die Prüfung so zu planen und durchzuführen, dass wir mit hinreichender Sicherheit beurteilen können, ob die Aussagen der gesetzlichen Vertreter zur Konzeption des CMS in der CMS-Beschreibung in allen wesentlichen Belangen zutreffend dargestellt sind und in der CMS-Beschreibung auf alle CMS-Grundelemente eingegangen wird.

Auftragsgemäß umfasste unsere Prüfung nicht die Beurteilung der Angemessenheit, Implementierung oder Wirksamkeit der Grundsätze und Maßnahmen (insb. des Compliance-

Programms und der Überwachungs- und Kommunikationsmaßnahmen) des CMS. Ein angemessener Prozess zur Konzeption eines CMS gewährleistet für sich genommen nicht, dass die implementierten Grundsätze und Maßnahmen angemessen und wirksam sind.

Die Auswahl der Prüfungshandlungen haben wir nach pflichtgemäßem Ermessen vorgenommen. Im Rahmen unserer Prüfung haben wir die Kenntnisse über das rechtliche und wirtschaftliche Umfeld und die Compliance-Anforderungen des Unternehmens berücksichtigt und auf dieser Grundlage Befragungen und eine Durchsicht von Organisationsunterlagen zum CMS vorgenommen. Wir haben die Inhalte in der CMS-Beschreibung sowie die uns vorgelegten Nachweise überwiegend auf der Basis von Stichproben beurteilt. Wir sind der Auffassung, dass unsere Prüfung eine hinreichend sichere Grundlage für unsere Beurteilung bildet.

Im Einzelnen haben wir folgende Prüfungshandlungen durchgeführt:

[Darstellung einzelner Prüfungshandlungen]

Wir haben die Prüfung (mit Unterbrechungen) in den Monaten ... bis zum ... durchgeführt.

Alle von uns erbetenen Aufklärungen und Nachweise sind erteilt worden. Die gesetzlichen Vertreter haben uns die Vollständigkeit und Richtigkeit der CMS-Beschreibung und der uns erteilten Aufklärungen und Nachweise zur Konzeption des CMS schriftlich bestätigt.

C. Feststellungen zum Compliance Management System

I. Konzeption des CMS für ... [Beschreibung des oder der abgegrenzten Teilbereiche(s)]

[unter anderem Nennung der angewandten CMS-Grundsätze]

Ausführungen zu den einzelnen CMS-Grundelementen:

- Compliance-Kultur
- Compliance-Organisation
- Compliance-Ziele
- Compliance-Risiken
- Compliance-Programm
- Compliance-Kommunikation
- Compliance-Überwachung und Verbesserung.

II. Feststellungen [und Empfehlungen]

[a) Feststellungen, die zu einer Einschränkung oder Versagung geführt haben

b) sonstige Feststellungen]

D. Prüfungsurteil

[ggf. Darstellung von bedeutenden Schwierigkeiten bei der Beurteilung des Prüfungsgegenstandes]

Nach unserer Beurteilung aufgrund der bei der Prüfung gewonnenen Erkenntnisse sind die in der CMS-Beschreibung enthaltenen Aussagen der gesetzlichen Vertreter zur Konzeption des CMS für ... [Beschreibung des oder der abgegrenzten Teilbereiche(s)] in allen wesentlichen Belangen zutreffend dargestellt. Die Beschreibung umfasst Aussagen zu sämtlichen Grundelementen eines CMS, insb. zur Compliance-Kultur, den Aufbau der Compliance-Organisation (Aufbau- und Ablauforganisation), die Festlegung der Compliance-Ziele, die Festlegung und Analyse der Compliance-Risiken durch das Unternehmen, den Prozess der Erstellung des Compliance-Programms, die Entwicklung des Kommunikationsprozesses sowie von Verfahren zur Überwachung und Verbesserung des CMS.

Zu unseren einzelnen Feststellungen [und Empfehlungen] verweisen wir auf unsere Ausführungen in [Abschn. C. II.].

Die CMS-Beschreibung der Gesellschaft für ... [Beschreibung des oder der abgegrenzten Teilbereiche(s)] wurde zum [Datum] erstellt. Jede Übertragung dieser Angaben auf einen zukünftigen Zeitpunkt birgt die Gefahr in sich, dass aufgrund von durchgeführten Änderungen die als Anlage beigefügte CMS-Beschreibung nicht dem aktuellen Stand entspricht.

Eine in Übereinstimmung mit den vom Unternehmen festgelegten CMS-Grundsätzen ... [Bezeichnung der CMS-Grundsätze] stehende Konzeption eines CMS gewährleistet alleine keine Sicherstellung eines regelkonformen Verhaltens des Unternehmens und seiner Mitarbeiter sowie ggf. Dritter.

Ort, Datum, Unterschrift

Anlagen:

[CMS-Beschreibung]

2.2. Auftragstyp 2

Bericht des unabhängigen Wirtschaftsprüfers

Die Prüfung der Angemessenheit und Implementierung des Compliance Management Systems für ... [Beschreibung des oder der abgegrenzten Teilbereiche(s)]

An die [Gesellschaft]

A. Prüfungsauftrag

Mit Schreiben vom [Datum] haben uns [die gesetzlichen Vertreter] der [Gesellschaft] beauftragt, eine Prüfung der in nachstehender Anlage 1 beigefügten CMS-Beschreibung der Angemessenheit und Implementierung ihres Compliance Management Systems für ... [Beschreibung des oder der abgegrenzten Teilbereiche(s)] durchzuführen.

Unter einem Compliance Management System (CMS) sind die Grundsätze und Maßnahmen eines Unternehmens zu verstehen, die auf die Sicherstellung eines regelkonformen Verhaltens des Unternehmens und seiner Mitarbeiter sowie ggf. Dritten abzielen, d.h. auf die Einhaltung bestimmter Regeln bzw. die Verhinderung von wesentlichen Verstößen gegen Regeln in abgegrenzten Teilbereichen (Regelverstöße). Unser Auftrag bezog sich auf die Beurteilung der Angemessenheit und Implementierung der in der als Anlage 1 beigefügten CMS-Beschreibung aufgeführten Grundsätze und Maßnahmen für ... [Beschreibung des oder der abgegrenzten Teilbereiche(s) des CMS].

Für die Durchführung des Auftrags und unsere Verantwortlichkeit sind, auch im Verhältnis zu Dritten, die diesem Bericht beigefügten Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 01.01.2002 vereinbart.

Über Art und Umfang sowie über das Ergebnis unserer Prüfung erstatten wir diesen Bericht, der ausschließlich an die Gesellschaft zur Verwendung für [interne Zwecke] gerichtet ist.

[alternativ: Wir erstellen diese Berichterstattung auf Grundlage des mit der ... [Gesellschaft] geschlossenen Auftrags, dem, auch mit Wirkung gegenüber Dritten, die beiliegenden Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 01.01.2002 mit der Maßgabe zugrunde liegen, dass die darin enthaltenen Haftungshöchstgrenzen allen Personen gegenüber, die diese Berichterstattung mit unserer vorherigen Zustimmung erhalten haben, gemeinschaftlich besteht.]

B. Gegenstand, Art und Umfang der Prüfung

Gegenstand unserer Prüfung waren die in der als Anlage 1 beigefügten CMS-Beschreibung enthaltenen Aussagen der gesetzlichen Vertreter über ... [Beschreibung des oder der abgegrenzten Teilbereiche(s) des CMS]. Die gesetzlichen Vertreter haben die CMS-Grundsätze [Bezeichnung der CMS-Grundsätze] zugrunde gelegt.

Die Verantwortung für das CMS einschließlich der Dokumentation des CMS und für den Inhalt der CMS-Beschreibung liegt bei den gesetzlichen Vertretern der Gesellschaft.

Unsere Aufgabe ist es, auf Grundlage der von uns durchgeführten Prüfung eine Beurteilung über die in der CMS-Beschreibung enthaltenen Aussagen der gesetzlichen Vertreter über die Angemessenheit und Implementierung der Grundsätze und Maßnahmen für ... [Beschreibung des oder der abgegrenzten Teilbereiche(s) des CMS] abzugeben. Die Beurteilung ist anhand der ... [Bezeichnung der CMS-Grundsätze] vorgenommen worden. Die Prüfung ist nicht darauf ausgerichtet, Prüfungssicherheit über die tatsächliche Einhaltung von Regeln zu erlangen.

Das für ... [Beschreibung des oder der abgegrenzten Teilbereiche(s)] implementierte CMS ist angemessen, wenn es mit hinreichender Sicherheit gewährleistet, dass Risiken für wesentliche Regelverstöße rechtzeitig erkannt und Verstöße verhindert werden. Zu einem angemessenen CMS zählt auch, dass bereits eingetretene Verstöße an die zuständige Stelle im Unternehmen zu berichten sind, damit die notwendigen Konsequenzen für eine Verbesserung des CMS getroffen werden.

Wir haben unsere Prüfung auf der Grundlage der für Wirtschaftsprüfer geltenden Berufspflichten unter Beachtung des *IDW Prüfungsstandards: Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen (IDW PS 980)* durchgeführt. Hiernach haben wir die Prüfung so zu planen und durchzuführen, dass wir mit hinreichender Sicherheit beurteilen können, ob die Aussagen der gesetzlichen Vertreter in der CMS-Beschreibung über die Grundsätze und Maßnahmen in allen wesentlichen Belangen zutreffend dargestellt sind, dass die dargestellten Grundsätze und Maßnahmen

- in Übereinstimmung mit den angewandten CMS-Grundsätzen ... [Bezeichnung der CMS-Grundsätze] geeignet sind, Risiken für wesentliche Verstöße gegen ... [Beschreibung der betreffenden Regeln bzw. des oder der abgegrenzten Teilbereiche(s)] mit hinreichender Sicherheit rechtzeitig zu erkennen und Verstöße zu verhindern und
- zum [Datum] implementiert sind.

Auftragsgemäß umfasste unsere Prüfung nicht die Beurteilung der Wirksamkeit der in der CMS-Beschreibung des Unternehmens dargestellten Grundsätze und Maßnahmen. Auch ein ansonsten wirksam erscheinendes CMS unterliegt systemimmanenten Grenzen, sodass möglicherweise auch wesentliche Regelverstöße auftreten können, ohne systemseitig verhindert oder aufgedeckt zu werden.

Die Auswahl der Prüfungshandlungen haben wir nach unserem pflichtgemäßen Ermessen vorgenommen. Im Rahmen unserer Prüfung haben wir die Kenntnisse über das rechtliche und wirtschaftliche Umfeld und die Compliance-Anforderungen des Unternehmens berücksichtigt. Wir haben die in der CMS-Beschreibung dargestellten Grundsätze und Maßnahmen sowie die uns vorgelegten Nachweise überwiegend auf der Basis von Stichproben beurteilt. Wir sind der Auffassung, dass unsere Prüfung eine hinreichend sichere Grundlage für unsere Beurteilung bildet.

Im Einzelnen haben wir folgende Prüfungshandlungen durchgeführt:

[Darstellung einzelner Prüfungshandlungen]

[Beschreibung von Aufbauprüfungen sowie der weiteren Prüfungshandlungen.]

Wir haben die Prüfung (mit Unterbrechungen) in den Monaten ... bis zum ... durchgeführt.

Alle von uns erbetenen Aufklärungen und Nachweise sind erteilt worden. Die gesetzlichen Vertreter haben uns die Vollständigkeit und Richtigkeit der CMS-Beschreibung und der uns erteilten Aufklärungen und Nachweise zur Konzeption des CMS sowie zur Angemessenheit und Implementierung schriftlich bestätigt.

C. Feststellungen zum Compliance Management System

I. Konzeption des CMS für ... [Beschreibung des oder der abgegrenzten Teilbereiche(s)]

[unter anderem Nennung der angewandten CMS-Grundsätze]

Ausführungen zu den einzelnen CMS-Grundelementen:

- Compliance-Kultur
- Compliance-Organisation
- Compliance-Ziele
- Compliance-Risiken
- Compliance-Programm
- Compliance-Kommunikation
- Compliance-Überwachung und Verbesserung.

II. Feststellungen [und Empfehlungen]

[a) Feststellungen, die zu einer Einschränkung oder Versagung führt haben

b) sonstige Feststellungen]

D. Prüfungsurteil

[ggf. Darstellung von bedeutenden Schwierigkeiten bei der Beurteilung des Prüfungsgegenstandes]

Nach unserer Beurteilung aufgrund der bei der Prüfung gewonnenen Erkenntnisse sind die Aussagen der gesetzlichen Vertreter in der CMS-Beschreibung über die Grundsätze und Maßnahmen des CMS in allen wesentlichen Belangen zutreffend dargestellt. Die in der CMS-Beschreibung dargestellten Grundsätze und Maßnahmen sind

- in Übereinstimmung mit den angewandten CMS-Grundsätzen ... [Bezeichnung der CMS-Grundsätze] geeignet, Risiken für wesentliche Verstöße gegen ... [Beschreibung der betreffenden Regeln bzw. des oder der abgegrenzten Teilbereiche(s)] mit hinreichender Sicherheit rechtzeitig zu erkennen und Verstöße zu verhindern und
- zum [Datum] implementiert.

Zu unseren einzelnen Feststellungen [und Empfehlungen] verweisen wir auf unsere Ausführungen in [Abschn. C. II.].

Die CMS-Beschreibung für ... [Beschreibung des oder der abgegrenzten Teilbereiche(s)] bei der Gesellschaft wurde zum [Datum] erstellt. Jede Übertragung dieser Angaben auf einen zukünftigen Zeitpunkt birgt die Gefahr in sich, dass aufgrund von durchgeführten Änderungen die als Anlage beigefügte CMS-Beschreibung des ... [Beschreibung des oder der abgegrenzten Teilbereiche(s)] nicht dem aktuellen Stand entspricht.

Ort, Datum, Unterschrift

Anlagen:

[CMS-Beschreibung]

2.3. Auftragstyp 3

Bericht des unabhängigen Wirtschaftsprüfers

Die Prüfung der Angemessenheit, Implementierung und Wirksamkeit des Compliance Management Systems für ... [Beschreibung des oder der abgegrenzten Teilbereiche(s)]

An die [Gesellschaft]

A. Prüfungsauftrag

Mit Schreiben vom [Datum] haben uns [die gesetzlichen Vertreter] der [Gesellschaft] beauftragt, eine Prüfung der in nachstehender Anlage 1 beigefügten CMS-Beschreibung der Angemessenheit, Implementierung und Wirksamkeit ihres Compliance Management Systems für ... [Beschreibung des oder der abgegrenzten Teilbereiche(s)] durchzuführen.

Unter einem Compliance Management System (CMS) sind die Grundsätze und Maßnahmen eines Unternehmens zu verstehen, die auf die Sicherstellung eines regelkonformen Verhaltens des Unternehmens und seiner Mitarbeiter sowie ggf. Dritten abzielen, d.h. auf die Einhaltung bestimmter Regeln bzw. die Verhinderung von wesentlichen Verstößen gegen Regeln in abgegrenzten Teilbereichen (Regelverstöße). Unser Auftrag bezog sich auf die Beurteilung der Angemessenheit, Implementierung und Wirksamkeit der in der als Anlage 1 beigefügten CMS-Beschreibung aufgeführten Grundsätze und Maßnahmen für ... [Beschreibung des oder der abgegrenzten Teilbereiche(s) des CMS].

Für die Durchführung des Auftrags und unsere Verantwortlichkeit sind, auch im Verhältnis zu Dritten, die diesem Bericht beigefügten Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 01.01.2002 vereinbart.

Über Art und Umfang sowie über das Ergebnis unserer Prüfung erstatten wir diesen Bericht, der ausschließlich an die Gesellschaft zur Verwendung für [interne Zwecke] gerichtet ist.

[alternativ: Wir erstellen diese Berichterstattung auf Grundlage des mit der ... [Gesellschaft] geschlossenen Auftrags, dem, auch mit Wirkung gegenüber Dritten, die beiliegenden Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 01.01.2002 mit der Maßgabe zugrunde liegen, dass die darin enthaltenen Haftungshöchstgrenzen allen Personen gegenüber, die diese Berichterstattung mit unserer vorherigen Zustimmung erhalten haben, gemeinschaftlich besteht.]

B. Gegenstand, Art und Umfang der Prüfung

Gegenstand unserer Prüfung waren die in der als Anlage 1 beigefügten CMS-Beschreibung enthaltenen Aussagen der gesetzlichen Vertreter über ... [Beschreibung des oder der abgegrenzten Teilbereich(e) des CMS]. Die gesetzlichen Vertreter haben die CMS-Grundsätze [Bezeichnung der CMS-Grundsätze] zugrunde gelegt.

Die Verantwortung für das CMS einschließlich der Dokumentation des CMS und für den Inhalt der CMS-Beschreibung liegt bei den gesetzlichen Vertretern der Gesellschaft.

Unsere Aufgabe ist es, auf Grundlage der von uns durchgeführten Prüfung eine Beurteilung über die in der CMS-Beschreibung enthaltenen Aussagen der gesetzlichen Vertreter über die Angemessenheit, Implementierung und Wirksamkeit des ... [Beschreibung des oder der abgegrenzten Teilbereiche(s) des CMS] abzugeben. Die Beurteilung ist anhand der ... [Bezeichnung der CMS-Grundsätze] vorgenommen worden. Die Prüfung ist nicht darauf ausgerichtet, Prüfungssicherheit über die tatsächliche Einhaltung von Regeln zu erlangen.

Das für ... [Beschreibung des oder der abgegrenzten Teilbereiche(s)] implementierte CMS ist angemessen, wenn es mit hinreichender Sicherheit gewährleistet, dass Risiken für wesentliche Regelverstöße rechtzeitig erkannt und Verstöße verhindert werden. Zu einem angemessenen CMS zählt auch, dass bereits eingetretene Verstöße an die zuständige Stelle im Unternehmen zu berichten sind, damit die notwendigen Konsequenzen für eine Verbesserung des CMS getroffen werden.

Die Wirksamkeit des CMS ist dann gegeben, wenn die Grundsätze und Maßnahmen von den hiervon Betroffenen nach Maßgabe ihrer Verantwortlichkeit zur Kenntnis genommen und beachtet werden.

Wir haben unsere Prüfung auf der Grundlage der für Wirtschaftsprüfer geltenden Berufspflichten unter Beachtung des *IDW Prüfungsstandards: Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen (IDW PS 980)* durchgeführt. Hiernach haben wir die Prüfung so zu planen und durchzuführen, dass wir mit hinreichender Sicherheit beurteilen können, ob die Aussagen der gesetzlichen Vertreter in der CMS-Beschreibung über die dargestellten Grundsätze und Maßnahmen in allen wesentlichen Belangen zutreffend dargestellt sind, dass die dargestellten Grundsätze und Maßnahmen

- in Übereinstimmung mit den angewandten CMS-Grundsätzen ... [Bezeichnung der CMS-Grundsätze] geeignet sind, Risiken für wesentliche Verstöße gegen ... [Beschreibung der betreffenden Regeln bzw. des oder der abgegrenzten Teilbereiche(s)] mit hinreichender Sicherheit rechtzeitig zu erkennen und Verstöße zu verhindern,
- zum [Datum] implementiert sind und
- während des Zeitraums vom [Datum] bis [Datum] wirksam waren und dadurch dazu beitragen, Risiken für wesentliche Regelverstöße mit hinreichender Sicherheit rechtzeitig zu erkennen und Verstöße zu verhindern.

Die Auswahl der Prüfungshandlungen haben wir nach unserem pflichtgemäßen Ermessen vorgenommen. Im Rahmen unserer Prüfung haben wir die Kenntnisse über das rechtliche

und wirtschaftliche Umfeld und die Compliance-Anforderungen des Unternehmens berücksichtigt. Wir haben die in der CMS-Beschreibung dargestellten Grundsätze und Maßnahmen sowie die uns vorgelegten Nachweise überwiegend auf der Basis von Stichproben beurteilt. Wir sind der Auffassung, dass unsere Prüfung eine hinreichend sichere Grundlage für unsere Beurteilung bildet.

Im Einzelnen haben wir folgende Prüfungshandlungen durchgeführt:

[Darstellung der Prüfungshandlungen]

[Beschreibung der Aufbau- und Funktionsprüfungen sowie der weiteren Prüfungshandlungen]

Wir haben die Prüfung (mit Unterbrechungen) in den Monaten ... bis zum ... durchgeführt.

Alle von uns erbetenen Aufklärungen und Nachweise sind erteilt worden. Die gesetzlichen Vertreter haben uns die Vollständigkeit und Richtigkeit der CMS-Beschreibung und der uns erteilten Aufklärungen und Nachweise zur Konzeption des CMS sowie zur Angemessenheit, Implementierung und Wirksamkeit schriftlich bestätigt.

C. Feststellungen zum Compliance Management System

I. Konzeption des CMS für ... [Beschreibung des oder der abgegrenzten Teilbereiche(s)]

[unter anderem Nennung der angewandten CMS-Grundsätze]

Ausführungen zu den einzelnen CMS-Grundelementen:

- Compliance-Kultur
- Compliance-Organisation
- Compliance-Ziele
- Compliance-Risiken
- Compliance-Programm
- Compliance-Kommunikation
- Compliance-Überwachung und Verbesserung.

II. Feststellungen [und Empfehlungen]

[a) Feststellungen, die zu einer Einschränkung oder Versagung geführt haben

b) sonstige Feststellungen]

D. Prüfungsurteil

[ggf. Darstellung von bedeutenden Schwierigkeiten bei der Beurteilung des Prüfungsgegenstandes]

Nach unserer Beurteilung aufgrund der bei der Prüfung gewonnenen Erkenntnisse sind die Aussagen der gesetzlichen Vertreter in der CMS-Beschreibung über die Grundsätze und Maßnahmen in allen wesentlichen Belangen zutreffend dargestellt. Die in der CMS-Beschreibung dargestellten Grundsätze und Maßnahmen sind

- in Übereinstimmung mit den angewandten CMS-Grundsätzen ... [Bezeichnung der CMS-Grundsätze] geeignet, Risiken für wesentliche Verstöße gegen ... [Beschreibung der betreffenden Regeln bzw. des oder der abgegrenzten Teilbereiche(s)] mit hinreichender Sicherheit rechtzeitig zu erkennen und Verstöße zu verhindern,
- zum [Datum] implementiert und
- waren während des Zeitraums vom [Datum] bis [Datum] wirksam und haben dadurch dazu beigetragen, Risiken für wesentliche Regelverstöße mit hinreichender Sicherheit rechtzeitig zu erkennen und Verstöße zu verhindern.

Zu unseren einzelnen Feststellungen [und Empfehlungen] verweisen wir auf unsere Ausführungen in [Abschn. C. II.].

Die CMS-Beschreibung des für ... [Beschreibung des oder der abgegrenzten Teilbereiche(s)] bei der Gesellschaft wurde zum [Datum] erstellt; die Ausführungen zu den Prüfungshandlungen zur Beurteilung der Wirksamkeit einzelner Grundsätze und Maßnahmen erstreckt sich auf den Zeitraum vom [Datum] bis [Datum]. Jede Übertragung dieser Angaben auf einen zukünftigen Zeitpunkt birgt die Gefahr in sich, dass aufgrund von durchgeführten Änderungen die als Anlage beigefügte CMS-Beschreibung des ... [Beschreibung des oder der abgegrenzten Teilbereiche(s)] nicht dem aktuellen Stand entspricht.

Auch ein ansonsten wirksam erscheinendes CMS unterliegt systemimmanenten Grenzen, sodass möglicherweise auch wesentliche Regelverstöße auftreten können, ohne systemseitig verhindert oder aufgedeckt zu werden.

Ort, Datum, Unterschrift

Anlagen:

[CMS-Beschreibung]

2.4. Auftragstyp 3 mit Einschränkung

Bericht des unabhängigen Wirtschaftsprüfers

Die Prüfung der Angemessenheit, Implementierung und Wirksamkeit des Compliance Management Systems für ... [Beschreibung des oder der abgegrenzten Teilbereiche(s)]

An die [Gesellschaft]

A. Prüfungsauftrag

Mit Schreiben vom [Datum] haben uns [die gesetzlichen Vertreter] der [Gesellschaft] beauftragt, eine Prüfung der in nachstehender Anlage 1 beigefügten CMS-Beschreibung der Angemessenheit, Implementierung und Wirksamkeit ihres Compliance Management Systems für ... [Beschreibung des oder der abgegrenzten Teilbereiche(s)] durchzuführen.

Unter einem Compliance Management System (CMS) sind die Grundsätze und Maßnahmen eines Unternehmens zu verstehen, die auf die Sicherstellung eines regelkonformen Verhaltens des Unternehmens und seiner Mitarbeiter sowie ggf. Dritten abzielen, d.h. auf die Einhaltung bestimmter Regeln bzw. die Verhinderung von wesentlichen Verstößen gegen Regeln in abgegrenzten Teilbereichen (Regelverstöße). Unser Auftrag bezog sich auf die Beurteilung der Angemessenheit, Implementierung und Wirksamkeit der in der als Anlage 1 beigefügten CMS-Beschreibung aufgeführten Grundsätze und Maßnahmen für ... [Beschreibung des oder der abgegrenzten Teilbereiche(s) des CMS].

Für die Durchführung des Auftrags und unsere Verantwortlichkeit sind, auch im Verhältnis zu Dritten, die diesem Bericht beigefügten Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 01.01.2002 vereinbart.

Über Art und Umfang sowie über das Ergebnis unserer Prüfung erstatten wir diesen Bericht, der ausschließlich an die Gesellschaft zur Verwendung für [interne Zwecke] gerichtet ist.

[alternativ: Wir erstellen diese Berichterstattung auf Grundlage des mit der ... [Gesellschaft] geschlossenen Auftrags, dem, auch mit Wirkung gegenüber Dritten, die beiliegenden Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 01.01.2002 mit der Maßgabe zugrunde liegen, dass die darin enthaltenen Haftungshöchstgrenzen allen Personen gegenüber, die diese Berichterstattung mit unserer vorherigen Zustimmung erhalten haben, gemeinschaftlich besteht.]

B. Gegenstand, Art und Umfang der Prüfung

Gegenstand unserer Prüfung waren die in der als Anlage 1 beigefügten CMS-Beschreibung enthaltenen Aussagen der gesetzlichen Vertreter über ... [Beschreibung des oder der abgegrenzten Teilbereiche(s) des CMS]. Die gesetzlichen Vertreter haben die CMS-Grundsätze [Bezeichnung der CMS-Grundsätze] zugrunde gelegt.

Die Verantwortung für das CMS einschließlich der Dokumentation des CMS und für den Inhalt der CMS-Beschreibung liegt bei den gesetzlichen Vertretern der Gesellschaft.

Unsere Aufgabe ist es, auf Grundlage der von uns durchgeführten Prüfung eine Beurteilung über die in der CMS-Beschreibung enthaltenen Aussagen der gesetzlichen Vertreter über die Angemessenheit, Implementierung und Wirksamkeit des ... [Beschreibung des oder der abgegrenzten Teilbereiche(s) des CMS] abzugeben. Die Beurteilung ist anhand der ... [Bezeichnung der CMS-Grundsätze] vorgenommen worden. Die Prüfung ist nicht darauf ausgerichtet, Prüfungssicherheit über die tatsächliche Einhaltung von Regeln zu erlangen.

Das für ... [Beschreibung des oder der Teilbereiche(s)] implementierte CMS ist angemessen, wenn es mit hinreichender Sicherheit gewährleistet, dass Risiken für wesentliche Regelver-

stöße rechtzeitig erkannt und Verstöße verhindert werden. Zu einem angemessenen CMS zählt auch, dass bereits eingetretene Verstöße an die zuständige Stelle im Unternehmen zu berichten sind, damit die notwendigen Konsequenzen für eine Verbesserung des CMS getroffen werden.

Die Wirksamkeit des CMS ist dann gegeben, wenn die Grundsätze und Maßnahmen von den hiervon Betroffenen nach Maßgabe ihrer Verantwortlichkeit zur Kenntnis genommen und beachtet werden.

Wir haben unsere Prüfung auf der Grundlage der für Wirtschaftsprüfer geltenden Berufspflichten unter Beachtung des *IDW Prüfungsstandards: Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen (IDW PS 980)* durchgeführt. Hiernach haben wir die Prüfung so zu planen und durchzuführen, dass wir mit hinreichender Sicherheit beurteilen können, ob die Aussagen der gesetzlichen Vertreter in der CMS-Beschreibung über die dargestellten Grundsätze und Maßnahmen in allen wesentlichen Belangen zutreffend dargestellt sind, dass die dargestellten Grundsätze und Maßnahmen

- in Übereinstimmung mit den angewandten CMS-Grundsätzen ... [Bezeichnung der CMS-Grundsätze] geeignet sind, Risiken für wesentliche Verstöße gegen ... [Beschreibung der betreffenden Regeln bzw. des oder der abgegrenzten Teilbereiche(s)] mit hinreichender Sicherheit rechtzeitig zu erkennen und Verstöße zu verhindern,
- zum [Datum] implementiert sind und
- während des Zeitraums vom [Datum] bis [Datum] wirksam waren und dadurch dazu beitragen, Risiken für wesentliche Regelverstöße mit hinreichender Sicherheit rechtzeitig zu erkennen und Verstöße zu verhindern.

Die Auswahl der Prüfungshandlungen haben wir nach unserem pflichtgemäßen Ermessen vorgenommen. Im Rahmen unserer Prüfung haben wir die Kenntnisse über das rechtliche und wirtschaftliche Umfeld und die Compliance-Anforderungen des Unternehmens berücksichtigt. Wir haben die in der CMS-Beschreibung dargestellten Grundsätze und Maßnahmen sowie die uns vorgelegten Nachweise überwiegend auf der Basis von Stichproben beurteilt. Wir sind der Auffassung, dass unsere Prüfung eine hinreichend sichere Grundlage für unsere Beurteilung bildet.

Im Einzelnen haben wir folgende Prüfungshandlungen durchgeführt:

[Darstellung der Prüfungshandlungen]

[Beschreibung der Aufbau- und Funktionsprüfungen sowie der weiteren Prüfungshandlungen]

Wir haben die Prüfung (mit Unterbrechungen) in den Monaten ... bis zum ... durchgeführt.

Alle von uns erbetenen Aufklärungen und Nachweise sind erteilt worden. Die gesetzlichen Vertreter haben uns die Vollständigkeit und Richtigkeit der CMS-Beschreibung und der uns erteilten Aufklärungen und Nachweise zur Konzeption des CMS sowie zur Angemessenheit, Implementierung und Wirksamkeit schriftlich bestätigt.

C. Feststellungen zum Compliance Management System

I. Konzeption des CMS für ... [Beschreibung des oder der abgegrenzten Teilbereiche(s)]

[u.a. Nennung der angewandten CMS-Grundsätze]

Ausführungen zu den einzelnen CMS-Grundelementen:

- Compliance-Kultur
- Compliance-Organisation
- Compliance-Ziele
- Compliance-Risiken
- Compliance-Programm
- Compliance-Kommunikation
- Compliance-Überwachung und Verbesserung.

II. Feststellungen [und Empfehlungen]

[a) Feststellungen, die zu einer Einschränkung geführt haben]

Da wir nur unzureichende Unterlagen und anderweitige Nachweise über die eingerichteten Maßnahmen für ... [Beschreibung des betreffenden Bereichs] erhalten haben, können wir die Angemessenheit und Wirksamkeit dieser Maßnahmen nicht beurteilen. Es kann daher nicht ausgeschlossen werden, dass das CMS insoweit nicht mit hinreichender Sicherheit gewährleistet, dass Risiken für wesentliche Regelverstöße mit hinreichender Sicherheit rechtzeitig erkannt und Verstöße verhindert werden.

[b) sonstige Feststellungen]

D. Prüfungsurteil

[ggf. Darstellung von bedeutenden Schwierigkeiten bei der Beurteilung des Prüfungsgegenstandes]

Unsere Prüfung hat zu der unter C. II. dargestellten Einschränkung geführt.

Mit dieser Einschränkung sind nach unserer Beurteilung aufgrund der bei der Prüfung gewonnenen Erkenntnisse die Aussagen der gesetzlichen Vertreter in der CMS-Beschreibung über die Grundsätze und Maßnahmen in allen wesentlichen Belangen zutreffend dargestellt. Die in der CMS-Beschreibung dargestellten Grundsätze und Maßnahmen sind

- in Übereinstimmung mit den angewandten CMS-Grundsätzen ... [Bezeichnung der CMS-Grundsätze] geeignet, Risiken für wesentliche Verstöße gegen ... [Beschreibung der betreffenden Regeln bzw. des oder der abgegrenzten Teilbereiche(s)] mit hinreichender Sicherheit rechtzeitig zu erkennen und Verstöße zu verhindern,
- zum [Datum] implementiert und

- waren während des Zeitraums vom [Datum] bis [Datum] wirksam und haben dadurch dazu beigetragen, Risiken für wesentliche Regelverstöße mit hinreichender Sicherheit rechtzeitig zu erkennen und Verstöße zu verhindern.

Zu unseren einzelnen Feststellungen [und Empfehlungen] verweisen wir auf unsere Ausführungen in [Abschn. C. II.].

Die CMS-Beschreibung für ... [Beschreibung des oder der abgegrenzten Teilbereiche(s)] bei der Gesellschaft wurde zum [Datum] erstellt; die Ausführungen zu den Prüfungshandlungen zur Beurteilung der Wirksamkeit einzelner Grundsätze und Maßnahmen erstreckt sich auf den Zeitraum vom [Datum] bis [Datum]. Jede Übertragung dieser Angaben auf einen zukünftigen Zeitpunkt birgt die Gefahr in sich, dass aufgrund von durchgeführten Änderungen die als Anlage beigefügte CMS-Beschreibung des ... [Beschreibung des oder der abgegrenzten Teilbereiche(s)] nicht dem aktuellen Stand entspricht.

Auch ein ansonsten wirksam erscheinendes CMS unterliegt systemimmanenten Grenzen, sodass möglicherweise auch wesentliche Regelverstöße auftreten können, ohne systemseitig verhindert oder aufgedeckt zu werden.

Ort, Datum, Unterschrift

Anlagen:

[CMS-Beschreibung]