Erfahrung nutzen, Zukunft sichern.

DIIR

Deutsches Institut für
Interne Revision e.V.

Ohmstraße 59
60486 Frankfurt am Main
Telefon (069) 713769-0
Fax (069) 713769-69
www.diir.de
info@diir.de

Geschäftsführer:
Wilfried Fischenich
Volker Hampel
USt-ID DE 114235123
Vereinsregisternummer:
Amtsgericht Frankfurt
am Main VR 5326

Stellungnahme des DIIR – Deutsches Institut für Interne Revision e. V. zum IDW EPS 980 – Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen

Mit der vorliegenden Stellungnahme möchte das DIIR – Deutsches Institut für Interne Revision e. V. Hinweise zur Optimierung des Entwurfs zum Prüfungsstandard „Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen (Stand: 11.03.2010)" geben.

Dabei wird unterschieden in einerseits „Allgemeine Anmerkungen", anhand derer Hinweise allgemeiner Natur zu Art, Umfang und Anwendbarkeit des Entwurfes des Prüfungsstandards gegeben werden.

Mit den Anmerkungen zu spezifischen Teilen des EPS 980 möchten wir darüber hinaus anhand konkreter Themen Anregungen zu inhaltlichen Anpassungen geben. Wo möglich, erfolgt dies anhand erläuternder Beispiele.

Allgemeine Anmerkungen

Der vorliegende Prüfungsstandard enthält wertvolle Hinweise, wie die Anforderungen an ein Compliance Management System in die Praxis transferiert werden können, indem sinnvolle strukturelle Komponenten hervorgehoben werden. Die – neben der fehlenden allgemeingültigen Definition für „Compliance" – in der Praxis sehr heterogenen Ausprägungen von Compliance Management Systemen führen allerdings zu erheblichen Interpretationsspielräumen hinsichtlich Angemessenheit und Wirksamkeit des zu betrachtenden Compliance Management Systems. Die parallele Etablierung eines CMS in Ergänzung zu oder in Überschneidung mit anderen Komponenten der Unternehmensüberwachung wie dem Internen Kontrollsystem (IKS) oder dem Risikomanagementsystem (RMS) führt zu erheblichen Abgrenzungsproblemen bzw. vermutlich auch Redundanzen. Sofern ein CMS – sollte es als eigenständiges Verfahren oder Organisation aufgefasst werden – lediglich zu einem zusätzlichen Aufwand ohne zusätzlichen Nutzen gegenüber dem IKS und RMS führen würde, wird es ohnehin schnell auf den Prüfstand gestellt werden müssen.

Die saubere Abgrenzung zu den vorgenannten Systemen bzw. Hinweise auf Überschneidungen – dies auch im Hinblick auf weitere PS des IDW – sollten deutlich stärker ausgeführt werden. Zusätzlich ist zu erwägen, ob über eine allgemeine Definition hinaus zumindest weiterführende Hilfestellungen im Hinblick auf die aktuell anzutreffende Unterscheidung nach:

a) der Abbildung über eigenständige organisatorische Komponenten („Compliance-Organisation" wie z. B. Compliance-Bereich oder -Abteilung)

b) der Abbildung in Form einer unternehmensinternen Projekt-ähnlichen Struktur

gegeben werden können. In beiden Fällen sind jeweils wichtige Fragen der bestehenden Verantwortlichkeiten und Prozesse zu beachten, die im Verlauf der eigentlichen Prüfung entscheidend für die Beurteilung der Angemessenheit und Wirksamkeit des Compliance Management Systems sein können. Gegebenenfalls kann hiermit eine Duplizierung bereits etablierter Kontrollprozesse vermieden werden.

Darüber hinaus sollten als Hilfsgrößen zur Beurteilung der Angemessenheit und Wirksamkeit des Compliance Management Systems (insbesondere im Hinblick auf die Erteilung eines uneingeschränkten Prüfungsergebnisses) typische qualitative Benchmarks aufgeführt werden, wo diese sinnvoll ausgewiesen werden können. Solche Parameter könnten sich bspw. auf spezifische Compliance-Organisationselemente oder spezifische Compliance-Prozesse beziehen und in diesem Zusammenhang exemplarische prozessbezogene Parameter definieren. Solche Parameter könnten dann typischerweise als geeignete Beurteilungsbasis sowie Stichprobengrundlage und -größe herangezogen werden.

An mehreren Stellen wird im vorliegenden IDW EPS 980 die Interne Revision in erster Linie als Informationsquelle genannt. Dies wird jedoch der Internen Revision nicht gerecht, da ihr Aufgabengebiet als wesentliches Element der Unternehmenskontrolle sehr umfassend ist. So kann durchaus die Prüfung eines Compliance Management Systems als solches eine ihrer standardmäßigen Kernaufgaben sein. Die Interne Revision wird damit auch in Fragen der Prüfung des Compliance Management Systems zu einem wichtigen Partner des Abschlussprüfers bei dessen Prüfung der Wirksamkeit und Angemessenheit des Compliance Management Systems.

Anmerkungen zu den einzelnen Gliederungspunkten des IDW EPS 980

Zu Kapitel 1. Vorbemerkungen

Tz. 1

Insgesamt kann unseres Erachtens der Eindruck entstehen, dass Compliance Management Systeme ein neues, u. U. zusätzliches und ggf. noch zu installierendes System erfordern. In aller Regel dürften aber CMS die Bestandsaufnahme, Systematisierung und Integration bestehender Prozeduren unter eventueller Ergänzung fehlender Bestandteile, nicht aber die Neukonzeption eines Systems umfassen.

Der Entwurf des IDW Prüfungsstandard 980 beschreibt das Compliance Management System als Teilbereich des unternehmensweiten Risikomanagements (Tz. 1). Damit berührt das Compliance Management System auch die Rechnungslegung, wird in diesem Zusammenhang vom Wirtschaftsprüfer geprüft und der Wirtschaftsprüfer berichtet hierzu (u. a. §§ 171 Abs. 1 AktG, 317 Abs. 4 HGB, 321 Abs. 4).

Die Abschlussprüfung grenzt sich gemäß Tz. A25 von der Compliance Management System-Prüfung dadurch ab, dass erstgenannte die Ordnungsmäßigkeit der Rechnungslegung beurteilt. Da u. a. das Konzept des allgemeinen Risikomanagements, die allgemeinen Standards und auch die evtl. eingesetzte Software die zuvor beschriebenen rechnungslegungsbezogenen Teilbereiche beinhalten sollten, ist unseres Erachtens eine Hilfe zur Abgrenzung der Geltungsbereiche des Compliance Management Systems und des Risikomanagementsystems sinnvoll. Ansonsten könnten ggf. Doppelarbeiten mit inkonsistenten Prüfungsergebnissen entstehen.

Möglicherweise könnten hierzu als Grundstruktur aus dem aktuellsten Lagebericht (Risikobericht) Abgrenzungsansätze für die in Frage kommenden Systeme entnommen werden.

Es sollte abgeleitet werden, wo Überschneidungen im Rahmen einer Prüfung des Risikomanagementsystems mit der Compliance Management System Prüfung zu erwarten sind bzw. wie diesen begegnet werden kann. Dies gilt einerseits für den typischen Prüfungsumfang und die Prüfungshandlungen im Rahmen der Abschlussprüfung sowie andererseits bei angesetzten oder beauftragten Verfahrensprüfungen, die ggf. auch im Zusammenhang mit der Abschlussprüfung beauftragt werden. Gleichzeitig führt dies zu der Anregung, ggf. bereits in Kapitel 5.2. des IDW EPS 980 „Mindestanforderungen" an die Dokumentation des zu prüfenden Compliance Management Systems zu definieren, um die folgende Prüfung und insbesondere Prüfungsfeststellungen hinreichend zu fundieren.

Zu Kapitel 2. Begriffsbestimmungen

2)a) Tz. 5

Der Begriff „Compliance" wird allgemein definiert. Die Beispiele in **Tz. A2** reichen von A bis Z (z. B. Außensteuerrecht bis Zollrecht). Hier wie in der Folge bei der Struktur der „Grundelemente eines CMS" in Kapitel 4 könnten weitere Abgrenzungen bzw. Detaillierungen vorgenommen werden. Für eine engere Abgrenzung und präzisere Definition kämen bspw. typische betriebliche Kernprozesse wie bspw. Einkauf, Materialwirtschaft oder Vertrieb in Betracht, also etwa

- beispielsweise Gesetze, Verträge, Richtlinien (wie angeführt); hier könnten konkrete Beispiele zur Verdeutlichung genannt werden
- Prozesse oder typische Prozesselemente, die üblicherweise oder häufig Betrachtungsgegenstand von Compliance-Erwägungen sind
- Überwachungselemente oder exemplarische Kontrollen, die in Compliance-relevanten Themenfeldern zum Einsatz kommen.

So könnte eine unterstützende Struktur geschaffen werden, auf die dann effizient bspw. die unter **A14** exemplarisch aufgeführten Kontrollen angewendet werden könnten. Ebenso kämen – jedoch ggü. den Kernprozessen mit nachrangiger Priorität – auch organisatorische Elemente eines Compliance Management Systems in Frage oder auch typische Aufgabenspektren, die mit der Compliance-Funktion verbunden sein können.

Die explizite Erwähnung vertraglicher Bestimmungen ist unseres Erachtens zu begrüßen, da neben den bestehenden Verfahren rechtlich bindende Sachverhalte nicht notwendig bei jedem Prüfungsansatz unmittelbar ersichtlich werden.

2)b) Tz. 6

Ein Compliance Management System i. S. d. IDW EPS 980 kann sich auf Geschäftsbereiche, auf operative Prozesse oder auf bestimmte Rechtsgebiete beziehen.

Diese Klausel in Verbindung mit der möglichen Limitierung des Prüfungsauftrags auf einen dieser Teilbereiche birgt die Gefahr einer unzureichenden Abdeckung des Prüfungsfeldes. In Verbindung mit unseren Ausführungen zu der Abgrenzung wesentlicher Elemente von Risikomanagement zu Compliance Management Systemen sollte erwogen werden, diese genannten Spezifikationen zum Gegenstand einer Auftragstypbestimmung zu machen. Unter Umständen kann dies sogar sinnvoller sein als die derzeitige Unterscheidung nach den Auftragstypen 1 bis 3. Gleichzeitig sollte beachtet und hervorgehoben werden, inwiefern eine Eingrenzung auf definierte Themenfelder unter Umständen die unternehmensweite Gesamtsicht

auf ein Compliance Management System nicht ermöglicht. Dies gilt insbesondere wegen der Wirkungszusammenhänge bzw. möglicherweise abweichenden Verantwortlichkeiten bei Teilsystemen ggü. dem Gesamtsystem.

2)c) Tz. 7

Hier sollte erwogen werden, eventuelle Mindestanforderungen an die Dokumentation des eingesetzten Compliance Management Systems anzusprechen. Für die Auftragsannahme und -durchführung ist dies unseres Erachtens essentiell. Allerdings sollte dabei auch ersichtlich werden, unter welchen (einschränkenden) Bedingungen ein nicht adäquat dokumentiertes CMS dennoch vom Abschlussprüfer untersucht werden kann. Es ist davon auszugehen, dass Unternehmen auch ohne ein formell ausgewiesenes CMS Compliance sinnvoll und wirkungsvoll betreiben könnten. Siehe hierzu auch **Tz. 23.**

2)d) Tz. 8 und Tz. 9

Die erwähnten allgemein anerkannten Rahmenkonzepte standardsetzender Organisationen sind unseres Erachtens in der derzeitigen Form nicht zielführend. Die unter **Tz. A4** und **Anlage 1** aufgeführten Konzepte referenzieren Rahmenkonzepte mit grundsätzlich unterschiedlichen Ansprüchen, was deren allgemeine Anwendbarkeit betrifft (unterschiedliche Betrachtungsgegenstände, unterschiedliche Schwerpunkte mit eingeschränkter Vergleichbarkeit). Die wahlweise Verwendung dieser unterschiedlichen Rahmenkonzepte kann unter Umständen zu abweichenden Prüfungsergebnissen führen. Unseres Erachtens wäre es sinnvoller, eines der Konzepte aufgrund seines strukturellen Ansatzes und der weltweiten Akzeptanz als exemplarischen Maßstab zu nennen und weitere Werke ergänzend für die Betrachtung weiterer oder auch spezifischer Themenfelder unter Verwendung dieses Konzeptes vorzuschlagen. Hierfür würde sich der mit COSO II dargestellte Ansatz ggf. anbieten.

2)e) Tz. 10

Hier sollte – wie bereits in Bezug auf Tz. 1 erwähnt – ein Hinweis zu Abgrenzung oder Kongruenz typischer Elemente des Compliance Management im Vergleich zu anderen Management Systemen wie Risikomanagement oder zum Internen Kontrollsystem eines Unternehmens gegeben werden. Die Hinweise müssten hierzu konkreter formuliert werden als derzeit noch unter **Tz. A11**, dritter Anstrich.

Zu Kapitel 3. Gegenstand, Ziel und Umfang der Prüfung

3)a) Tz. 14a

Hier sollte erwogen werden, einen Halbsatz „... und die wesentlichsten organisatorischen Belange abgebildet, die notwendigen Verantwortlichkeiten definiert und die erforderlichen Kompetenzen nachvollziehbar erteilt wurden." anzufügen. Kerngedanke ist es, die nachfolgend in **Tz. 19** referenzierten Grundelemente eines CMS auch hinsichtlich deren Angemessenheit und Wirksamkeit tatsächlich nachvollziehen zu können.

3)b) Tz. 14b und Tz. 16

„Verstöße verhindern" ist eine Anforderung aus der Tz. 14b und der Tz. **16**. An anderer Stelle wird richtigerweise von „Verstöße vermeiden" gesprochen (**Tz. 19** „Compliance-Programm", **Tz. A8** „Hinreichende Sicherheit"). Es sollte zumindest durchgängig in dem IDW EPS 980 ein Ausdruck verwendet werden. Dabei sollte beachtet werden, dass eine „Verhinderung mit hinreichender Sicherheit" eine ggf. nur schwer zu erfüllende Erwartungshaltung generieren könnte.

Die angesprochenen Risiken gemäß **Tz. 16** könnten verbal ggf. auf solche Risiken eingegrenzt werden, die nachvollziehbar unter die Abdeckung des betrachteten CMS fallen bzw. explizit in der Abgrenzung für das betrachtete CMS relevant sind.

Der Aspekt der Wesentlichkeit bezieht sich lediglich auf das Erkennen von (wesentlichen) Verstößen. Die Verhinderung, Berichterstattung und das Ergreifen von Konsequenzen beziehen sich im IDW EPS 980 wiederholt auf „Verstöße" ohne Einschränkung auf die Wesentlichkeit. Es sollte erwogen werden, bei Erkennung und Berichterstattung konsistent vorzugehen bzw. explizit eine Differenzierung zu definieren.

3)c) Tz. 17

Die Wirksamkeit des CMS ist dann gegeben, wenn die Betroffenen die Grundsätze und Maßnahmen zur Kenntnis genommen haben und diese beachten: es sollte erwogen werden, ob die Definition der Wirksamkeit anhand folgender Fragestellungen präzisiert werden kann:

- Welche exemplarischen Fälle einer Nichtbeachtung führen zum Urteil „Unwirksamkeit des Compliance Management Systems"?
- Sind alle Grundsätze und Maßnahmen der Compliance Management System-Beschreibung des Unternehmens für die Beurteilung relevant oder lediglich die wesentlichen?

- In den Grundelementen eines Compliance Management Systems wird in **Tz. 19** auch die Überwachung der Wirksamkeit durch das Unternehmen gefordert. Hier sollte die Konsistenz der Betrachtungsgegenstände aus der eigenen Compliance-Überwachung des Unternehmens mit derjenigen des externen Prüfers betrachtet werden, damit ggf. abweichende Urteile „greifbarer" werden.

3)d) Tz. 18

In Ergänzung zu den Ausführungen sollte erwogen werden, mögliche Voraussetzungen für die Prüfbarkeit eines Compliance Management Systems zu nennen. In Frage kommen die Nachvollziehbarkeit der Compliance-Kommunikation durch die Unternehmensleitung, unterschiedlichste Organisations- und Prozessdokumentationen etc. In Anbetracht der Komplexität der Materie sollte Wert auf eine angemessene Dokumentation gelegt werden. Dies gilt für alle Elemente des CMS; besonders wichtig erscheint jedoch die nachvollziehbare und aktuelle Berücksichtigung der relevanten Compliance-Risiken, um hinsichtlich der Angemessenheit und Wirksamkeit des CMS geeignete Untersuchungen vornehmen zu können.

Zu Kapitel 4. Grundelemente eines CMS

4)a) Tz. 19

Beim Grundelement „Compliance-Risiken" sollte die Abgrenzung zu den bereits bestehenden Risikomanagement-Systemen erfolgen. Hier ist unter Umständen zu klären, ob es sich bei Compliance-Risiken in aller Regel um Risiken handelt, die nicht bereits auch über das Risikomanagement-System in ggf. anderer Weise berücksichtigt werden. Dann wäre auf das bestehende Risikomanagementsystem als Quelle zur systematischen Risikoerkennung und Berichterstattung zu verweisen. Sind Compliance-Risiken im Sinne des EPS 980 hingegen anders geartet, sollte eine entsprechende Definition hier erfolgen. Zusätzlich ist dann zu empfehlen, diese Definition auch bereits unter Kapitel 2 „Begriffsbestimmungen" zu verwenden.

Unter dem Punkt „Compliance-Kommunikation" sollte die Interne Revision grundsätzlich als Adressat der Berichterstattung von Compliance-Risiken und Hinweisen von Regelverstößen aufgenommen werden. Insgesamt sollte darauf hingewiesen werden, dass in Form der Berichterstattungsprozesse der Internen Revision bereits Kommunikationswege bestehen, die vergleichbar auch im Zusammenhang mit einem CMS verwendet werden könnten. Dies erfordert ebenfalls die eindeutige Zuordnung von Verantwortlichkeiten.

Für die „Compliance-Überwachung und Verbesserung" muss die Interne Revision Erwähnung finden. Nach ihrem Aufgabenfeld, der risikoorientierten Prüfungsplanung und insbesondere durch ihren Prüfungsansatz ist die Interne Revision die prädestinierte interne Kontrollinstanz für die Überprüfung von CMS. Dies sollte auch in **Tz. A16** deutlicher hervorgehoben werden.

Zudem ist die Angemessenheit und Wirksamkeit des Compliance Management Systems in geeigneter Weise durch das Unternehmen zu überwachen (Tz. 19). Gemäß Tz. A16 ist die Compliance-Überwachung durch eine prozessunabhängige Stelle, z. B. die Interne Revision durchzuführen. Sollten diese Ausführungen sich lediglich auf die Einhaltung einzelner Compliance-Maßnahmen unter Tz. A16 und nicht auf das CMS als solches beziehen, stimmen wir diesen Ausführungen nicht zu. Im Rahmen eines allgemeinen Risikomanagementsystems sind die Prozesse zur Überwachung als Bestandteil des Internen Kontrollsystems einzuordnen und gehören demnach in den Verantwortungsbereich des operativen Managements (s. u. a. KWG § 25a, COSO). Ein zentrales Risikomanagement oder ein zentraler Compliance-Bereich hätte die notwendigen Standards für die Überwachung der Wirksamkeit durch die operativen Bereiche zu definieren. Eine prozessunabhängige Stelle wie die Interne Revision hat in risikoorientierten und stichprobenhaften Prüfungen die Wirksamkeit der Überwachung durch die operativen Bereiche zu beurteilen.

Ist also unter Tz. A16 das CMS gemeint, sollten entsprechende Anpassungen vorgenommen werden.

Zu Kapitel 5.2. Prüfungsanforderungen – Auftragsannahme

5)a) Tz. 24

Siehe hierzu auch unsere Ausführungen zu Tz. 7.

5)b) Tz. 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."

Dies steht unseres Erachtens im Widerspruch zum Auftragstyp 3 „Prüfung von Angemessenheit, Implementierung und Wirksamkeit des CMS" (Tz. 14c). Es stellt sich die Frage, wie die Wirksamkeit des CMS ohne Überprüfung der tatsächlichen Einhaltung von Regeln geprüft werden kann. Dies gilt umso mehr, als dass „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." Sollte in Tz. 26 eine Beschränkung auf eine durch die Aussagen der gesetzlichen Vertreter abgegrenzte Grundmenge angestrebt sein, so sollte hier alternativ formuliert werden. Andernfalls bedingt

schon die Beurteilung der von den gesetzlichen Vertretern getroffenen Aussagen zur Wirksamkeit des CMS eine Prüfung der Regeleinhaltung.

Zu Kapitel 5.3.1. Prüfungsanforderungen – Prüfungsplanung – Allgemeine Grundsätze

5)c) Tz. 28

Bei dieser Tz. sollte erwogen werden – sofern dies im EPS 980 nicht direkt unter den Terminus „Systemprüfungen" gefasst wird – zusätzlich Erfahrungen bei Risikomanagement- und Verfahrens-Prüfungen zu ergänzen.

5)d) Tz. 30

Unseres Erachtens kann das Prüfungsrisiko nicht ausschließlich auf die Begrenzung wesentlicher Fehler in den Aussagen der gesetzlichen Vertreter abstellen. Vielmehr können Beurteilungen der Wirksamkeit und der Angemessenheit des Compliance Management Systems durch Auswahl einer unzureichenden Grundmenge oder Stichprobe wie auch auf einer unzureichenden risikoorientierten Planung im Rahmen der Prüfung basieren.

5)e) Tz. 34

Die Bestimmung der Wesentlichkeit liegt gemäß **Tz. 34** im Ermessen des Prüfers des Compliance Management Systems. Dabei ist eine Herleitung der Wesentlichkeit nicht trivial.

Es stellt sich die Frage, ob sich die Wesentlichkeit gemäß § 91 Abs. 2 AktG auf den Fortbestand der Gesellschaft gefährdende Entwicklungen beschränkt oder ob im Rahmen eines Compliance Management Systems Straftatbestände oder auch anderweitige Verfehlungen als wesentliche Verstöße anzusehen sind. An dieser Stelle sollten konkrete Kriterien aufgeführt werden, anhand derer die Wesentlichkeit eingestuft werden kann. Denkbar wäre hier neben qualitativen Kriterien bspw. ein Vorschlag hinsichtlich der Risikohöhe oder ein Bezug auf „Materiality-„ Werte, wie sie auch bei SOX-Prüfungen angewendet werden.

Zu Kapitel 5.4. Prüfungsanforderungen – Prüfungsdurchführung

5)f) Tz. 35

Prüfungsgegenstand des Wirtschaftsprüfers sind die Aussagen der gesetzlichen Vertreter in der Compliance Management System-Beschreibung. Im Fokus steht dabei im Wesentlichen die vom Unternehmen selbst erstellte Compliance Management System-Beschreibung.

Es ist fraglich, ob im Rahmen der Prüfung gemäß IDW EPS 980 ein im Ist-Zustand funktionsfähiges Compliance Management System festgestellt werden könnte, wenn im Wesentlichen

lediglich Schwächen in der Compliance Management System-Beschreibung – dem Soll – vorliegen würden. Dies gilt insbesondere für den Auftragstyp 3. Hier könnte auch ein Widerspruch zu **Tz. 42** vorliegen, die konkrete Funktionsprüfungen anspricht. Insofern sollte auch auf die Konsistenz der **Tz. 26** und **Tz. 42** besonderes Augenmerk gelegt werden.

Zu Kapitel 5.4.3.1. Prüfungsanforderungen – Prüfungsdurchführung – Weitere Prüfungshandlungen – Festgestellte Regelverstöße

5)g) Tz. 44

Wird ein Mangel oder ein Rechtsverstoß festgestellt, so sollte auch geprüft werden, ob und wie die gesetzlichen Vertreter diesen abstellen. Dabei ist es wichtig, dass die Reaktion zeitnah erfolgt. Die Reaktion auf den Regelverstoß sollte insofern selbst Prüfungsobjekt sein.

Zu Kapitel 6. Anwendungshinweise und Erläuterungen – Grundelemente eines CMS (Tz. 19) – Compliance-Kultur

6)a) Tz. A10

Es könnte erwogen werden, im Besonderen auf den Stellenwert einzugehen, den die gesetzlichen Vertreter den Kontrollorganen wie der Internen Revision im Zuge der Compliance-Kultur beimessen. Im abschließenden Satz wird zwar auf Sanktionen eingegangen, es könnten allerdings neben den Anreizsystemen auch die Kontroll- und Präventionssysteme oder -elemente explizit aufgeführt werden.

Bei einzelnen Punkten kann zudem erwogen werden, Beispiele anzuführen, anhand derer die angeführten Punkte konkreter nachvollzogen werden können. Beispielsweise könnte geprüft werden, ob ein schriftliches, kommuniziertes Bekenntnis des Managements zur Bedeutung eines verantwortungsvollen Verhaltens im Einklang mit den zu beachtenden Regeln vorliegt.

Zu Kapitel 6. Anwendungshinweise und Erläuterungen – Grundelemente eines CMS (Tz. 19) – Compliance-Organisation

6)b) Tz. A11

Es sollte darauf geachtet werden, dass durch die Formulierungen nicht der Eindruck nach der Forderung einer expliziten Organisation der Compliance in Form eines Bereiches oder einer Abteilung entsteht. Compliance kann genauso über eine Projektorganisation wie ggf. unter dem Begriff „Compliance-Gremium" gewährleistet werden.

Zu Kapitel 6. Anwendungshinweise und Erläuterungen – Grundelemente eines CMS (Tz. 19) – Compliance-Überwachung und Verbesserung

Aufgrund ihrer Bedeutung als wichtige prozessunabhängige Instanz sollte die Interne Revision stärker hervorgehoben werden. Nicht nur prüft die Interne Revision ohnehin wesentliche Prozesse und Verfahren neben der Rechnungslegung, sondern ggf. auch das CMS. Darüber hinaus verfügt die Interne Revision über Standards und Prozeduren, mit denen sie auch die Erkenntnisse aus Prüfungen gezielt kommuniziert und insbesondere im Rahmen der Überwachung erkannte Schwachstellen durch etablierte Prozeduren einer Verbesserung zuführen kann („Follow-up").

Außerdem sollte der Aufzählungspunkt „Entwicklung eines Überwachungsplans" ergänzt werden durch „in Abstimmung mit dem Jahresprüfprogramm und der Prüfungsplanung der Internen Revision".

Zu Kapitel 6. Anwendungshinweise und Erläuterungen – Prüfungsdurchführung (Tz. 35)

6)c) Tz. A24

Unseres Erachtens kann ein wesentlicher Aspekt im Fehlen klarer Verantwortlichkeiten sowie auch der fehlenden Gewährleistung angemessener Kompetenzen liegen. Es sollte erwogen werden, dies wie auch die Überprüfung der Sicherstellung der Compliance-relevanten Kenntnisse und fachlichen Qualifikationen der Führungskräfte und Mitarbeiter aufzunehmen.

Zu Kapitel Anlagen, hier: 2. Berichterstattung über CMS-Prüfungen

In „2. Berichterstattung über CMS-Prüfungen" wird unter „B. Gegenstand, Art und Umfang der Prüfung" für alle 3 Auftragstypen darauf verwiesen, die Prüfung sei nicht darauf ausgerichtet, Prüfungssicherheit über die tatsächliche Einhaltung von Regeln zu erlangen.

Diese Formulierung führt unter Umständen zu der Annahme, dass keine Prüfungshandlungen vorgenommen werden, die eine Aussage zur Einhaltung der Regeln ermöglichen würden.

Für den beschriebenen Auftragstyp 1 (Konzept) kann dies nachvollzogen werden.

Zur Beurteilung der Angemessenheit und der Implementierung des Compliance Management Systems (Auftragstyp 2) sowie zusätzlich der Wirksamkeit (Auftragstyp 3) sollte erwogen werden, auch ausreichende Prüfungshandlungen zum Nachweis einer angemessenen Einhaltung der Regeln vorzusehen.

Zusammenfassung

Der Eindruck, CMS seien ein vollständig neues Thema und müssten parallel zu den bestehenden Elementen des Risikomanagements und des Internen Kontrollsystems eingerichtet werden, sollte vermieden werden. Die Überwachung der Ordnungsmäßigkeit und des IKS ist grundsätzlich über die Interne Revision etabliert.

Die Abgrenzung bzw. Darstellung der Überschneidungen zwischen den Prüfungshandlungen im Rahmen der Jahresabschlussprüfung und zusätzlicher freiwilliger Prüfungen gemäß IDW EPS 980 sollten präzisiert werden.

Bei der Beschreibung der erforderlichen Prüfungsanforderungen zum Nachweis der Angemessenheit und Wirksamkeit des Compliance Management Systems sollten im IDW EPS 980 zusätzliche Konkretisierungen erfolgen und Praxisbeispiele soweit möglich die konkreten Fragestellungen als Anleitung erläutern.

Die Bedeutung der Internen Revision im Kontext von Compliance und ihre Aufgabe, die Funktionsfähigkeit des Überwachungssystems zu prüfen, sollte hervorgehoben werden.