Entwurf einer Neufassung des IDW Prüfungsstandards: Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen (IDW EPS 980 n.F. (10.2021))

Stand: 28.10.2021[1]

Der Hauptfachausschuss (HFA) des IDW hat den nachfolgenden Entwurf einer Neufassung des IDW Prüfungsstandards: Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen (IDW EPS 980 n.F. (10.2021)) verabschiedet.

Die Überarbeitung des IDW PS 980 ist insb. aus folgenden Gründen erforderlich geworden:

Seit der Veröffentlichung des IDW PS 980 im Jahr 2011 haben sich bei der Einrichtung und Prüfung von Compliance Management Systemen (CMS) Fortentwicklungen in der Unternehmens- und Prüfungspraxis ergeben, die entsprechend bei der Überarbeitung der Grundelemente eines CMS und der Prüfungsdurchführung berücksichtigt wurden. So haben sich z.B. neue CMS-Rahmenkonzepte oder -standards etabliert, die in die Überarbeitung eingeflossen sind.

- *Die sich aus dem Gesetz zur Stärkung der Finanzmarktintegrität (Finanzmarktintegritätsstärkungsgesetz – FISG) ergebenden Änderungen in Bezug auf die Einrichtungspflichten von internen Kontroll- und Risikomanagementsystemen wurden bei der Überarbeitung berücksichtigt.*
- *In der Rechtsprechung haben sich Weiterentwicklungen im Bereich „Compliance" ergeben. So wurde in dem BGH-Urteil vom 09.05.2017 (1 StR 265/16) anerkannt, dass bei der Bemessung einer Geldbuße gegen ein Unternehmen zu berücksichtigen ist, ob es im Zeitpunkt von Gesetzesverstößen ein angemessenes und effektives Compliance Management System installiert hatte. In die Bußgeldbemessung ist auch einzubeziehen, ob das Unternehmen im Zuge der Aufklärung der Non-Compliance zu Tage getretene Defizite des Compliance Management Systems behebt und Maßnahmen ergreift, um vergleichbare Normverletzungen in Zukunft zu verhindern oder zumindest wesentlich zu erschweren. Im Entwurf wird diesbezüglich hervorgehoben, dass zum Nachweis der jederzeitigen Angemessenheit des CMS im Zeitablauf und der kontinuierlichen Anwendung der Regelungen die Dokumentation unbeschadet von Aufbewahrungspflichten über einen ausreichend langen Zeitraum aufbewahrt werden sollte (vgl. Tz. A18).*
- *Der HFA hat im Nachgang zur Veröffentlichung des IDW PS 980 weitere IDW Prüfungsstandards zur Prüfung von Risikomanagementsystemen (IDW PS 981), zur Prüfung des internen Kontrollsystems des internen und externen Berichtswesens (IDW PS 982) sowie zur Prüfung von Internen Revisionssystemen (IDW PS 983) verabschiedet. IDW*

[1] Vorbereitet vom Arbeitskreis „Prüfungsfragen und betriebswirtschaftliche Fragen zu Governance, Risk und Compliance" (GRC). Verabschiedet vom Hauptfachausschuss (HFA) am 11.03.2011. Neufassung zur Berücksichtigung der Fortentwicklungen bei der Einrichtung und Prüfung von CMS; vorbereitet von Arbeitskreis „GRC", verabschiedet vom HFA am 28.10.2021.

EPS 980 n.F. berücksichtigt Änderungen, die sich aus dem Zusammenwirken dieser IDW Prüfungsstandards ergeben.

- *Die bisher noch vorgesehene Auftragsart einer sogenannten Konzeptionsprüfung, die ausschließlich auf die angemessene Darstellung der in der CMS-Beschreibung enthaltenen Aussagen zur Konzeption des CMS abstellt, hat in der Praxis keine Bedeutung mehr und ist daher in der überarbeiteten Fassung nicht mehr enthalten.*
- *Bei der Überarbeitung der Prüfungsanforderungen und Anwendungshinweise wurde die zwischenzeitlich überarbeitete Fassung des International Standard on Assurance Engagements (ISAE) 3000 (Revised) „Assurance Engagements Other than Audits or Reviews of Historical Financial Information" zugrunde gelegt.*

Änderungs- oder Ergänzungsvorschläge zu dem Entwurf werden schriftlich an die Geschäftsstelle des IDW (Postfach 32 05 80, 40420 Düsseldorf oder stellungnahmen@idw.de) bis zum 31.05.2022 erbeten. Die Änderungs- oder Ergänzungsvorschläge werden im Internet auf der IDW Website 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.

1. Einleitung

1.1. 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 planen und durchführen sowie darüber Bericht erstatten.

2 Gemäß § 91 Abs. 3 AktG hat der Vorstand einer börsennotierten Gesellschaft über ein Risikofrüherkennungssystem nach § 91 Abs. 2 AktG hinaus auch ein im Hinblick auf den Umfang der Geschäftstätigkeit und die Risikolage des Unternehmens angemessenes und wirksames internes Kontrollsystem und Risikomanagementsystem einzurichten (vgl. Tz. A1). Das interne

Kontroll- und Risikomanagementsystem umfasst die Grundsätze, Verfahren und Maßnahmen zur Sicherung der Wirksamkeit und Wirtschaftlichkeit der Geschäftstätigkeit, zur Sicherung der Ordnungsmäßigkeit der Rechnungslegung und zur Sicherung der Einhaltung der maßgeblichen rechtlichen Vorschriften (Compliance).[2]

3 Die Einhaltung der gesetzlichen Vorschriften gehört zu den Organisations- und Sorgfaltspflichten der gesetzlichen Vertreter. Nach der Rechtsprechung hat der Vorstand im Rahmen seiner Legalitätspflicht dafür Sorge zu tragen, dass das Unternehmen so organisiert und beaufsichtigt wird, dass Gesetzesverstöße verhindert werden. Seiner Organisationspflicht genügt ein Vorstandsmitglied bei entsprechender Gefährdungslage dann, wenn es eine auf Schadensprävention und Risikokontrolle angelegte Compliance-Organisation einrichtet. Die Einhaltung des Legalitätsprinzips und demgemäß die Einrichtung eines funktionierenden Compliance Management Systems gehört zur Gesamtverantwortung des Vorstands.[3] Einem angemessenen und wirksamen Compliance Management System kommt aus Sicht des Unternehmens nicht nur präventive Wirkung zu, sondern ein Compliance Management System kann im Falle eines eingetretenen Compliance-Regelverstoßes auch eine bußgeldmindernde Wirkung entfalten.[4]

4 § 107 Abs. 3 Satz 2 AktG sieht vor, dass der Aufsichtsrat aus seiner Mitte einen Prüfungsausschuss bestellen kann, der sich neben der Überwachung der Abschlussprüfung befasst mit

- der Überwachung des Rechnungslegungsprozesses,
- der Wirksamkeit
  - des internen Kontrollsystems,
  - des Risikomanagementsystems und
  - des internen Revisionssystems (vgl. Tz. A2 ff.).

5 Die Überwachungsaufgaben des Aufsichtsrats umfassen auch die Maßnahmen des Vorstands, die sich auf die Begrenzung der Risiken aus möglichen Verstößen gegen gesetzliche Vorschriften und interne Richtlinien (Compliance) beziehen. Dem trägt die Empfehlung D.3. des Deutschen Corporate Governance Kodex (DCGK) Rechnung, der zu den Aufgaben des Prüfungsausschusses ausführt, dass sich der Prüfungsausschuss – falls kein anderer Ausschuss damit betraut ist – auch mit der Compliance des Unternehmens befasst.

6 Eine Prüfung der Wirksamkeit dieser Systeme durch einen unabhängigen Wirtschaftsprüfer nach diesem *IDW Prüfungsstandard* kann dem objektivierten Nachweis der ermessensfehlerfreien Ausübung der Organisations- und Sorgfaltspflichten des Vorstands und des Aufsichtsrats dienen.

7 Dieser *IDW Prüfungsstandard* behandelt die Prüfung des Teils des unternehmensweiten Risikomanagements, der auf die Einhaltung von Regeln im Unternehmen (vgl. Tz. 14) ausgerichtet ist (Compliance Management System; CMS). Die Prüfung i.S. dieses *IDW Prüfungsstandards* umfasst stets sämtliche Grundelemente des CMS (vgl. Tz. 27). Eine isolierte Prüfung einzelner Grundelemente liegt nicht im Anwendungsbereich dieses *IDW Prüfungsstandards* (vgl. Tz. A6).

---

[2] Vgl. Gesetzesbegründung zum Bilanzrechtsmodernisierungsgesetzes (BilMoG), BT-Drucks. 16/10067, S. 77.

[3] Vgl. sogenanntes „Neubürger-Urteil“ (LG München I, Urteil vom 10.12.2013 – 5HK O 1387/10).

[4] Vgl. BGH, 09.05.2017 – 1 StR 265/16.

8 Sofern in diesem *IDW Prüfungsstandard* die Begriffe „CMS“ oder „CMS-Prüfung“ verwendet werden, beziehen sich diese auf die von den gesetzlichen Vertretern bestimmten Teilbereiche des CMS (vgl. Tz. 13d) und Tz. A7), die einer CMS-Prüfung unterliegen sollen.

9 Für die Prüfung des Risikomanagementsystems, des internen Kontrollsystems der Unternehmensberichterstattung sowie des Internen Revisionssystems hat das IDW gesonderte *IDW Prüfungsstandards* veröffentlicht.[5] Die Abgrenzung der Prüfungsgegenstände ist dabei nicht notwendigerweise überschneidungsfrei. In Abhängigkeit von den Prüfungszielen und der Festlegung des zu prüfenden Teilbereichs durch die gesetzlichen Vertreter können deshalb mehrere dieser Verlautbarungen bei einem Prüfungsauftrag anwendbar sein.

10 Neben Definitionen (Abschn. 1.2.), Gegenstand, Ziel und Umfang der Prüfung (Abschn. 1.3.) und einer Beschreibung der Grundelemente eines CMS (Abschn. 2.) enthält dieser *IDW Prüfungsstandard* in dem Abschn. 3. zu beachtende Prüfungsanforderungen sowie Anwendungshinweise und Erläuterungen (Abschn. 4. und Anlagen).[6]

11 Dieser *IDW Prüfungsstandard* behandelt Prüfungsaufträge zur Erlangung hinreichender Sicherheit. Dem *IDW Prüfungsstandard* liegt der International Standard on Assurance Engagements (ISAE) 3000 (Revised) „Assurance Engagements Other than Audits or Reviews of Historical Financial Information“ (Dezember 2013)[7] zugrunde. Ein Verweis im CMS-Prüfungsbericht auf die ergänzende Beachtung des ISAE 3000 (Revised) ist nicht vorgesehen und würde die Beachtung etwaiger zusätzlicher einschlägiger Anforderungen des ISAE 3000 (Revised) erfordern.

12 Dieser *IDW Prüfungsstandard* ist erstmals anzuwenden bei freiwilligen Prüfungen von CMS, die nach dem 31.12.2022 beauftragt werden.[8]

1.2. Definitionen

13 Für die Zwecke dieses *IDW Prüfungsstandards* gelten die folgenden Begriffsdefinitionen:

a) *Compliance* – Einhaltung von Regeln (gesetzliche Bestimmungen und unternehmensinterne Richtlinien (vgl. Tz. A8)).

b) *Compliance Management System* – die auf der Grundlage der von den gesetzlichen Vertretern festgelegten Ziele eingeführten Regelungen eines Unternehmens, die auf ein

---

5 Vgl. *IDW Prüfungsstandard: Grundsätze ordnungsmäßiger Prüfung von Risikomanagementsystemen (IDW PS 981)* (Stand: 03.03.2017), *IDW Prüfungsstandard: Grundsätze ordnungsmäßiger Prüfung des internen Kontrollsystems des internen und externen Berichtswesens (IDW PS 982) (Stand: 03.03.2017) und IDW Prüfungsstandard: Grundsätze ordnungsmäßiger Prüfung von Internen Revisionssystemen (IDW PS 983) (Stand: 03.03.2017).*

6 Die Anwendungshinweise und sonstigen Erläuterungen (einschließlich der Anlagen) enthalten weiterführende Hinweise zu den Anforderungen dieses *IDW Prüfungsstandards* sowie zu deren Umsetzung. Insbesondere können sie
a) genauer erläutern, was eine Anforderung bedeuten oder abdecken soll;
b) Beispiele für Prüfungshandlungen enthalten, die unter den gegebenen Umständen geeignet sein können.
Obwohl solche erläuternden Hinweise keine Anforderungen darstellen, sind sie für die richtige Anwendung der Anforderungen dieses *IDW Prüfungsstandards* relevant.

7 https://www.iaasb.org/publications/international-standard-assurance-engagements-isae-3000-revised-assurance-engagements-other-audits-or-0 (letzter Aufruf: 19.11.2021).

8 Eine freiwillige frühere Anwendung dieses *IDW Prüfungsstandards* ist zulässig.

regelkonformes Verhalten der gesetzlichen Vertreter und der Mitarbeiter des Unternehmens sowie ggf. von Dritten abzielen, d.h. auf die Einhaltung bestimmter Regeln und damit auf die Verhinderung von wesentlichen Verstößen (Regelverstöße) (vgl. Tz. A9 ff.).

c) *Regelungen* – Oberbegriff für Grundsätze, Verfahren und vorgegebene Maßnahmen im Rahmen des CMS.

d) *Teilbereich* – von den gesetzlichen Vertretern abgegrenzter Teil des CMS, der einer Prüfung nach diesem *IDW Prüfungsstandard* unterliegt (vgl. Tz. A7).

e) *CMS-Grundsätze* – Anforderungen an das CMS, die das Unternehmen aus allgemein anerkannten Rahmenkonzepten oder aus anderen angemessenen Rahmenkonzepten ableitet oder die vom Unternehmen selbst entwickelt werden (vgl. Tz. A12, A22 und 32).

f) *Allgemein anerkannte Rahmenkonzepte für CMS* – Rahmenkonzepte, 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. A13 und Anlage 1).

g) *CMS-Beschreibung* – Beschreibung der Regelungen zu den Grundelementen eines CMS für einen oder mehrere zu prüfende(n) Teilbereich(e) des CMS. Die angewandten CMS-Grundsätze werden in der CMS-Beschreibung entweder durch Verweis auf eine allgemein zugängliche Quelle (z.B. auf eine öffentlich zugängliche Website einer standardsetzenden Organisation) oder durch Nennung der einzelnen Grundsätze konkretisiert (vgl. Tz. A14).

h) *Prüfungsrisiko* – Risiko, dass der CMS-Prüfer ein uneingeschränktes Prüfungsurteil abgibt, wenn die CMS-Beschreibung wesentliche falsche Darstellungen aufweist.

i) *Falsche Darstellung in der CMS-Beschreibung* – die CMS-Beschreibung ist unvollständig oder enthält falsche oder irreführende Darstellungen (vgl. Tz. A15).

j) *Mangel des CMS* – Das CMS ist nicht in der Lage, mit hinreichender Sicherheit sowohl Risiken für wesentliche Verstöße gegen die Regeln, auf deren Einhaltung das zu prüfende CMS ausgerichtet ist, rechtzeitig zu erkennen als auch solche Regelverstöße zu verhindern.

k) *Sachverständiger des CMS-Prüfers* – eine natürliche Person oder eine Organisation mit Fachkenntnissen auf einem anderen Gebiet als betriebswirtschaftlichen Prüfungen, deren Arbeit auf diesem Gebiet vom CMS-Prüfer genutzt wird, um den CMS-Prüfer dabei zu unterstützen, ausreichende geeignete Prüfungsnachweise zu erlangen. Bei einem Sachverständigen des CMS-Prüfers handelt es sich entweder um einen internen Sachverständigen (d.h. einen Partner oder fachlichen Mitarbeiter der Praxis des CMS-Prüfers oder eines Mitglieds des Netzwerks der Wirtschaftsprüferpraxis) oder um einen externen Sachverständigen des CMS-Prüfers.

14 Für die Zwecke dieses *IDW Prüfungsstandards* umfasst der Begriff „Unternehmen“ nicht nur Unternehmen im rechtlichen Sinne, sondern auch andere Einheiten (vgl. Tz. A16).

1.3. Gegenstand, Ziel und Umfang der Prüfung

15 Gegenstand der Prüfung sind die in einer CMS-Beschreibung enthaltenen Darstellungen der gesetzlichen Vertreter des Unternehmens in Bezug auf die zu prüfenden Teilbereiche.

16 Es liegt nicht in der Verantwortung des CMS-Prüfers, die Abgrenzung der Teilbereiche durch die gesetzlichen Vertreter zu beurteilen (vgl. Tz. 43). Die Verantwortung für das CMS und die Inhalte der CMS-Beschreibung einschließlich der Abgrenzung der Teilbereiche, die der Prüfung unterliegen sollen, sowie für die Auswahl bzw. Entwicklung geeigneter CMS-Grundsätze 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 Aufstellung der CMS-Beschreibung durch geeignete Personen im Unternehmen, z.B. den Compliance-Beauftragten (vgl. Tz. A17 f.).

17 Ziel einer Wirksamkeitsprüfung des CMS ist es, dass der CMS-Prüfer hinreichende Sicherheit darüber erlangt, ob

- die im geprüften Zeitraum implementierten (vgl. Tz. 24) Regelungen des CMS in der CMS-Beschreibung in Übereinstimmung mit den angewandten CMS-Grundsätzen in allen wesentlichen Belangen angemessen dargestellt (vgl. Tz. 22) sind,
- die dargestellten Regelungen in Übereinstimmung mit den angewandten CMS-Grundsätzen in allen wesentlichen Belangen
  - während des geprüften Zeitraums geeignet waren, mit hinreichender Sicherheit sowohl Risiken für wesentliche Regelverstöße rechtzeitig zu erkennen als auch solche Regelverstöße zu verhindern, und
  - während des geprüften Zeitraums wirksam (vgl. Tz. 25) waren.

18 Anstelle einer Prüfung der Wirksamkeit ist die Beauftragung einer Prüfung möglich, die sich nur auf die Angemessenheit und Implementierung der in der CMS-Beschreibung dargestellten Regelungen des CMS bezieht (Angemessenheitsprüfung). Eine Wirksamkeitsprüfung umfasst stets auch die Angemessenheitsprüfung.

19 Die Angemessenheitsprüfung zielt darauf ab, dass der CMS-Prüfer hinreichende Sicherheit darüber erlangt, ob

- die zu einem bestimmten Zeitpunkt implementierten Regelungen des CMS in der CMS-Beschreibung in Übereinstimmung mit den angewandten CMS-Grundsätzen in allen wesentlichen Belangen angemessen dargestellt sind,
- die dargestellten Regelungen in Übereinstimmung mit den angewandten CMS-Grundsätzen in allen wesentlichen Belangen
  - geeignet sind, mit hinreichender Sicherheit sowohl Risiken für wesentliche Regelverstöße rechtzeitig zu erkennen als auch solche Regelverstöße zu verhindern, und
  - zu einem bestimmten Zeitpunkt implementiert (vgl. Tz. 24) waren.

20 Für Unternehmen, die ein CMS erstmals einrichten oder erweitern, ist es zulässig, im Rahmen einer Angemessenheitsprüfung einen CMS-Prüfer bereits während der Entwicklung, Einführung, Änderung oder Erweiterung des Systems projektbegleitend mit der CMS-Prüfung nach diesem *IDW Prüfungsstandard* zu beauftragen (vgl. Tz. A19).

21 Die Zielsetzung einer nach diesem *IDW Prüfungsstandard* durchgeführten Prüfung liegt als Systemprüfung nicht in dem Erkennen von einzelnen Regelverstößen. Sie ist daher nicht darauf ausgerichtet, Prüfungssicherheit über die tatsächliche Einhaltung von Regeln zu erlangen (vgl. Tz. 35).

22 Die in der CMS-Beschreibung enthaltenen Aussagen zu den Regelungen des CMS sind angemessen dargestellt, wenn sie auf sämtliche der in Tz. 27 genannten Grundelemente eines CMS eingehen und keine wesentlichen falschen Darstellungen (vgl. Tz. 13i)) enthalten.

23 Die Regelungen des CMS sind angemessen, wenn sie geeignet sind, mit hinreichender Sicherheit sowohl Risiken für wesentliche Regelverstöße rechtzeitig zu erkennen als auch solche Regelverstöße zu verhindern. Hierzu zählt auch, dass bereits eingetretene Regelverstöße zeitnah an die zuständige Stelle im Unternehmen zu berichten sind, damit die notwendigen Konsequenzen für eine Verbesserung des CMS getroffen werden (vgl. Tz. A20).

24 Der Begriff Implementierung bezieht sich auf die Einrichtung der Regelungen in den Geschäftsprozessen zu einem bestimmten Zeitpunkt.

25 Die Wirksamkeit des CMS ist dann gegeben, wenn die als angemessen beurteilten Regelungen in den laufenden Geschäftsprozessen von den hiervon betroffenen Personen nach Maßgabe ihrer Verantwortung in einem bestimmten Zeitraum wie vorgesehen eingehalten werden (vgl. Tz. A21).

26 Es liegt in der Verantwortung des CMS-Prüfers, Prüfungshandlungen durchzuführen, um ausreichende geeignete Prüfungsnachweise zu erlangen, auf die er sein Urteil zu den in der CMS-Beschreibung enthaltenen Darstellungen stützen kann.

2. Grundelemente eines CMS

27 Ein CMS i.S. dieses *IDW Prüfungsstandards* weist die folgenden miteinander in Wechselwirkung stehenden Grundelemente auf, die in die Geschäftsabläufe eingebunden sind. Die Konzeption des CMS berücksichtigt die Wechselwirkungen zwischen den Grundelementen (vgl. Tz. A22 ff.). Die konkrete Ausgestaltung des CMS hängt insb. von den festgelegten Compliance-Zielen, der Größe des Unternehmens, der vorherrschenden Unternehmenskultur sowie von Art, Umfang und Komplexität der Geschäftstätigkeit des Unternehmens ab:

Compliance-Kultur (vgl. Tz. A23)	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 im Umgang mit Compliance Risiken („tone at the top“), die Rolle der für die Überwachung Verantwortlichen sowie die Art und Weise, wie das Management die zentralen Unternehmenswerte und die weiteren Grundelemente in der Organisation verankert. Die Compliance-Kultur beeinflusst maßgeblich die Bedeutung, welche die Mitarbeiter des Unternehmens der Beachtung von Regeln beimessen und damit die Bereitschaft zu regelkonformem Verhalten.

Compliance-Ziele (vgl. Tz. A24)	Die gesetzlichen Vertreter legen auf der Grundlage der allgemeinen Unternehmensziele, der daraus abgeleiteten Unternehmensstrategie 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 Regelungsbereiche des CMS und der in den einzelnen Bereichen einzuhaltenden Regeln. Die Compliance-Ziele stellen die Grundlage für die Beurteilung von Compliance-Risiken dar.
Compliance-Risiken (vgl. Tz. A25)	Unter Berücksichtigung der Compliance-Ziele werden die Compliance-Risiken identifiziert, die Verstöße gegen einzuhaltende Regeln und damit eine Verfehlung der Compliance-Ziele zur Folge haben können. Hierzu wird ein Verfahren zur systematischen Risikoidentifikation und -bewertung eingeführt. Die identifizierten Risiken werden im Hinblick auf Eintrittswahrscheinlichkeit und mögliche Folgen analysiert, wobei mögliche Risikointerdependenzen berücksichtigt werden.
Compliance-Programm (vgl. Tz. A26)	Auf der Grundlage der Beurteilung der Compliance-Risiken werden Regelungen 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 im Hinblick auf eine personenunabhängige Funktion des CMS dokumentiert.
Compliance-Organisation (vgl. Tz. A27)	Die gesetzlichen Vertreter regeln die Rollen und Verantwortlichkeiten (Aufgaben) sowie Aufbau- und Ablauforganisation im CMS als integralen Bestandteil der Unternehmensorganisation und stellen die für ein wirksames CMS notwendigen Ressourcen zur Verfügung. Verantwortungsbereiche und Rollen sind klar abgegrenzt, kommuniziert und dokumentiert. Die Aufgabenträger erfüllen die erforderlichen persönlichen und fachlichen Voraussetzungen. Die wesentlichen Regelungen zur Aufbau- und Ablauforganisation des Compliance-Managements sind dokumentiert und verbindlich vorgegeben.
Compliance-Kommunikation (vgl. Tz. A28)	Die jeweils betroffenen Mitarbeiter und ggf. Dritte werden über die Compliance-Kultur, das Compliance-Programm sowie die festgelegten Rollen und Verantwortlichkeiten informiert und hierzu in einem strukturierten Ansatz sensibilisiert sowie aus- und weitergebildet, damit sie 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. die gesetzlichen Vertreter und erforderlichenfalls das Aufsichtsorgan) berichtet werden.
Compliance-Überwachung und Verbesserung (vgl. Tz. A29)	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 nach erfolgter Ursachenanalyse Schwachstellen im CMS bzw. Regelverstöße 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.

3. Anforderungen

3.1. Berufspflichten

28 CMS-Prüfungen i.S. dieses *IDW Prüfungsstandards* sind betriebswirtschaftliche Prüfungen außerhalb der Abschlussprüfung, bei denen der CMS-Prüfer neben den allgemeinen Berufspflichten der Unabhängigkeit, Verschwiegenheit, Eigenverantwortlichkeit und Gewissenhaftigkeit (§§43 Abs. 1 Satz 1, 44, 49 und 50 WPO, §§ 1 – 12 BS WP/vBP) auch die besonderen Berufspflichten nach §§ 28 – 44 BS WP/vBP zu beachten hat.

3.2. Auftragsannahme

29 Vor Auftragsannahme hat sich der CMS-Prüfer zu vergewissern, dass die Regelungen des Qualitätssicherungssystems der WP-Praxis zur Auftragsannahme und Auftragsfortführung eingehalten werden.[9] Ein Auftrag zur Durchführung einer CMS-Prüfung darf nur angenommen werden, wenn davon auszugehen ist, dass die relevanten Berufspflichten einschließlich des Unabhängigkeitsgrundsatzes eingehalten werden können. Dies setzt voraus, dass ausreichende Erfahrung und Kompetenz sowie personelle und zeitliche Ressourcen in der WP-Praxis vorhanden sind oder erlangt werden können, um den Auftrag ordnungsgemäß durchführen zu können (§ 4 Abs. 2 BS WP/vBP).

30 Die Durchführung der Abschlussprüfung für das Unternehmen steht einer Beauftragung als CMS-Prüfer nicht entgegen.

31 Bei der notwendigen Beurteilung der Auftragsrisiken vor Auftragsannahme hat der CMS-Prüfer festzustellen, ob das vorgesehene Prüfungsteam insgesamt über die für die Durchführung des Auftrags notwendigen Fach- und Branchenkenntnisse verfügt, sofern erforderlich Erfahrungen mit den einschlägigen rechtlichen Anforderungen vorliegen oder erlangt werden können, und erforderlichenfalls Sachverständige (z.B. forensische Experten oder IT-Spezialisten bei der Beurteilung der Sicherheit von IT-gestützten Prozessen im Rahmen der Prüfung des CMS) zur Verfügung stehen.[10] Zudem hat der CMS-Prüfer festzustellen, ob er davon ausgehen kann, dass die erforderlichen Prüfungsnachweise erlangt werden.

32 Im Zusammenhang mit der Entscheidung über die Annahme eines Auftrags zur Durchführung einer CMS-Prüfung hat sich der CMS-Prüfer Informationen über die Ausgestaltung des CMS und die Eignung 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. 27 dargestellten Grundelemente eines CMS zu erfolgen. Vom Unternehmen selbst entwickelte und verwendete CMS-Grundsätze hat der CMS-Prüfer stets auf Eignung zu beurteilen (vgl. Tz. A30 ff.).

33 Da die Grundlage der Prüfung eine Beschreibung des im Unternehmen eingerichteten CMS ist, darf der Prüfer den Auftrag nur annehmen, wenn eine CMS-Beschreibung vorliegt bzw. die gesetzlichen Vertreter ihre Bereitschaft erklären, eine CMS-Beschreibung aufzustellen.

---

[9] Vgl. *IDW Qualitätssicherungsstandard: Anforderungen an die Qualitätssicherung in der Wirtschaftsprüferpraxis (IDW QS 1)* (Stand: 09.06.2017), Tz. 70 ff. sowie Tz. 115.

[10] Vgl. *IDW QS 1*, Tz. 75.

34 Der CMS-Prüfer hat mit dem Auftraggeber die Auftragsbedingungen – einschließlich der Verantwortlichkeiten der gesetzlichen Vertreter und des CMS-Prüfers – schriftlich zu vereinbaren (vgl. Tz. A34 ff.).

35 Im Auftragsbestätigungsschreiben ist darauf hinzuweisen, dass keine Prüfungssicherheit über die tatsächliche Einhaltung von Regeln erlangt wird, sondern ausschließlich die in der CMS-Beschreibung getroffenen Darstellungen zum CMS und die Angemessenheit und Wirksamkeit der in der CMS-Beschreibung dargestellten Regelungen beurteilt werden (vgl. Tz. 21).

36 Wird dem CMS-Prüfer vor Auftragsannahme ein Prüfungshemmnis bekannt, das nach Einschätzung des CMS-Prüfers zu einer Erklärung der Nichtabgabe des Prüfungsurteils führen würde, darf er den Auftrag nicht annehmen.

37 Werden dem CMS-Prüfer nach Auftragsannahme Informationen bekannt, die – wenn sie ihm vorher bekannt geworden wären – zur Ablehnung des Auftrags geführt hätten, hat er über die erforderlichen Schritte zu entscheiden, z.B. bei Unabhängigkeitsgefährdungen die Ergreifung von Schutzmaßnahmen i.S. von § 30 BS WP/vBP oder ggf. die Niederlegung des Mandats.[11]

38 Der CMS-Prüfer darf nach Auftragsannahme einer Änderung der Bedingungen des Prüfungsauftrags nicht zustimmen, wenn es dafür keine vertretbare Begründung gibt (vgl. Tz. A37). Erfolgt eine Änderung der Bedingungen, darf der Prüfer Prüfungsnachweise nicht außer Acht lassen, die vor der Änderung der Auftragsbedingungen erlangt wurden.

3.3. Prüfungsplanung

3.3.1. Allgemeine Grundsätze

39 Der CMS-Prüfer hat die Prüfung in sachlicher, personeller und zeitlicher Hinsicht so zu planen, dass eine ordnungsgemäße Prüfungsdurchführung möglich ist. Hierzu sind Art, zeitliche Einteilung und Umfang der geplanten Prüfungshandlungen festzulegen, die erforderlich sind, um die Prüfungsziele (vgl. Tz. 17 ff.) zu erreichen.

40 Bei der Auswahl der Mitglieder des Prüfungsteams hat der CMS-Prüfer darauf zu achten, dass diese insgesamt über ausreichende praktische Erfahrungen mit Systemprüfungen sowie die notwendigen Branchen- und ggf. Rechtskenntnisse verfügen, um den Auftrag ordnungsgemäß durchzuführen und ein sachgerechtes Prüfungsurteil zu erteilen.[12] Das Prüfungsteam muss über ausreichende Kenntnisse der Anforderungen verfügen, auf deren Einhaltung das CMS abzielt. Erforderlichenfalls sind Sachverständige hinzuzuziehen (vgl. Tz. A38).

41 Bei der Hinzuziehung von Sachverständigen hat sich der CMS-Prüfer zu vergewissern, dass das Prüfungsteam im erforderlichen Umfang in die Tätigkeit des Sachverständigen eingebunden werden kann, um die Verantwortung für sein Prüfungsurteil insgesamt übernehmen zu können.

42 Der CMS-Prüfer muss die Prüfung mit einer kritischen Grundhaltung[13] planen und mit dem Bewusstsein durchführen, dass Umstände bestehen können, die dazu führen, dass das CMS zu dem zu prüfenden Zeitpunkt bzw. in dem zu prüfenden Zeitraum nicht angemessen bzw.

---

[11] Vgl. *IDW QS 1*, Tz. 79 f.

[12] Vgl. § 38 Abs. 3 BS WP/vBP.

[13] Zur kritischen Grundhaltung vgl. ISAE 3000 (Revised), Tz. 12 (u).

wirksam war. Unter Ausübung seines pflichtgemäßen Ermessens hat der CMS-Prüfer die Prüfungshandlungen so zu planen und durchzuführen, dass das Prüfungsrisiko (vgl. Tz. 13h)) so weit reduziert wird, um mit hinreichender Sicherheit beurteilen zu können, ob die CMS-Beschreibung wesentliche falsche Darstellungen (vgl. Tz. 47) enthält.

43 Bei der Bestimmung von Art und Umfang der Prüfungshandlungen hat der CMS-Prüfer die Art des Prüfungsauftrags (Angemessenheits- oder Wirksamkeitsprüfung) und das beurteilte Risiko wesentlicher falscher Darstellungen in der CMS-Beschreibung (vgl. Abschn. 3.3.3) zu berücksichtigen, das insb. von den angewandten CMS-Grundsätzen, der Beschreibung des CMS durch die gesetzlichen Vertreter und den in der CMS-Beschreibung dargestellten Teilbereichen des CMS bestimmt wird. Hierbei ist es nicht Aufgabe des Prüfers, zu beurteilen, welche Regelungsbereiche von den gesetzlichen Vertretern als Gegenstand der unternehmensweiten Compliance-Organisation festgelegt bzw. welche Teilbereiche als Gegenstand einer CMS-Prüfung abgegrenzt wurden. Der CMS-Prüfer hat jedoch bei der Prüfungsplanung und -durchführung darauf zu achten, dass die Abgrenzung und Darstellung des zu prüfenden Teilbereichs keine Irreführung der Berichtsadressaten zur Folge hat (vgl. Tz. 90 und A31).

44 Der CMS-Prüfer muss die geplanten Prüfungshandlungen in einem Prüfungsprogramm zusammenfassen, das die Prüfungsanweisungen zur sachlichen und zeitlichen Auftragsabwicklung für die Mitglieder des Prüfungsteams enthält.

45 Zudem hat der CMS-Prüfer die auftragsbezogenen Qualitätssicherungsmaßnahmen zu planen einschließlich der Überwachung der Auftragsabwicklung und der Durchsicht der Prüfungsergebnisse.[14]

46 Bei der Planung und Durchführung der Prüfungshandlungen hat der CMS-Prüfer die Relevanz und Verlässlichkeit der Informationen zu berücksichtigen, die als Prüfungsnachweis verwendet werden sollen (vgl. Tz. A39). Falls:

- die aus einer Quelle gewonnenen Prüfungsnachweise nicht mit den aus einer anderen Quelle gewonnenen Prüfungsnachweisen vereinbar sind oder
- der CMS-Prüfer Zweifel an der Zuverlässigkeit von Informationen hat, die als Prüfungsnachweis verwendet werden sollen,

hat er festzustellen, ob und welche Änderungen oder Ergänzungen der Prüfungshandlungen erforderlich sind, um die Inkonsistenzen bzw. Zweifel zu beseitigen, und etwaige Auswirkungen auf andere Aspekte der Prüfung zu berücksichtigen.

3.3.2. Wesentlichkeit

47 Der CMS-Prüfer hat für Zwecke der Planung und Durchführung der Prüfungshandlungen Wesentlichkeitsüberlegungen anzustellen. In diesem Rahmen hat der CMS-Prüfer zu beurteilen, in welchen Fällen eine festgestellte falsche Darstellung in der CMS-Beschreibung bzw. in welchen Fällen ein festgestellter Mangel des CMS als wesentlich einzustufen ist (vgl. Tz. A40 ff.). Die Bestimmung der Wesentlichkeit liegt im pflichtgemäßen Ermessen des CMS-Prüfers.

[14] Vgl. *IDW QS 1*, Tz. 107 ff., 133 ff.

3.3.3. Prüfungshandlungen zur Identifikation und Beurteilung von Risiken wesentlicher falscher Darstellungen in der CMS-Beschreibung

3.3.3.1. Gewinnung eines Verständnisses von dem Unternehmen sowie von dessen rechtlichem und wirtschaftlichem Umfeld

48 Der CMS-Prüfer hat unter Berücksichtigung der Umstände des gegebenen Auftrags (vgl. Abschn. 3.2 und Tz. 43) ein Verständnis von dem rechtlichen und wirtschaftlichen Umfeld, den Merkmalen des Unternehmens sowie den Unternehmenszielen und -strategien zu erlangen, soweit dies für den bzw. die zu prüfenden Teilbereich(e) des CMS relevant ist.

49 Das zu erlangende Verständnis muss – unter Berücksichtigung der in Abschn. 3.3.3.2 dargestellten Prüfungshandlungen – ausreichen, um die Risiken wesentlicher falscher Darstellungen in der CMS-Beschreibung bzw. Risiken wesentlicher Mängel des in der CMS-Beschreibung dargestellten CMS (vgl. Tz. A44) festzustellen und zu beurteilen. Das erlangte Verständnis muss zudem eine angemessene Grundlage bilden für die Planung und Durchführung von Prüfungshandlungen als Reaktion auf die festgestellten und beurteilten Risiken und zur Erlangung hinreichender Sicherheit für die Bildung des Prüfungsurteils (vgl. Tz. A45 f.).

3.3.3.2. Gewinnung eines Verständnisses von dem in der CMS-Beschreibung dargestellten CMS

50 Der CMS-Prüfer muss ein angemessenes Verständnis von dem in der CMS-Beschreibung dargestellten CMS erlangen. Hierzu gehört, dass sich der CMS-Prüfer u.a. durch Befragungen ein angemessenes Verständnis von den Verantwortlichkeiten sowie über die Prozesse und internen Kontrollen zur Aufstellung der CMS-Beschreibung verschafft (vgl. Tz. A48). Dies umfasst die Beurteilung der Konzeption und Einrichtung der für die Aufstellung der CMS-Beschreibung relevanten Kontrollen.

51 Der CMS-Prüfer hat ferner Befragungen der gesetzlichen Vertreter sowie weiterer geeigneter Personen im Unternehmen durchzuführen,

- ob diese Personen Kenntnisse über vorliegende, vermutete oder behauptete bewusst falsche Darstellungen in der CMS-Beschreibung oder Mängel des CMS haben,
- ob das Unternehmen über eine Interne Revision verfügt; falls eine solche eingerichtet ist, sind weitere Befragungen durchzuführen, um sich ein Verständnis von den Aktivitäten und bedeutsamen Feststellungen der Internen Revision in Bezug auf das zu prüfende CMS zu machen (vgl. Tz. 70 f.) und
- ob das Unternehmen Sachverständige bei der Konzeption des CMS oder der Aufstellung der CMS-Beschreibung eingesetzt hat (vgl. Tz. 69).

3.3.3.3. Identifizierung und Beurteilung der Risiken wesentlicher falscher Darstellungen in der CMS-Beschreibung

52 Der CMS-Prüfer muss auf der Grundlage des gewonnenen Verständnisses von dem Unternehmen und von dessen rechtlichem und wirtschaftlichem Umfeld sowie von dem zu prüfenden CMS die Risiken wesentlicher falscher Darstellungen in der CMS-Beschreibung identifizieren und beurteilen. Auf dieser Grundlage hat der CMS-Prüfer weitere Prüfungshandlungen

zur Prüfung der Angemessenheit und sofern einschlägig der Wirksamkeit des CMS zu planen und durchzuführen.

53 Sofern der CMS-Prüfer im Rahmen der Prüfungsdurchführung Nachweise erlangt, die mit den Prüfungsnachweisen nicht in Einklang stehen, auf die er seine Risikobeurteilung ursprünglich gestützt hat, muss er die Risikobeurteilung anpassen und die weiteren geplanten Prüfungshandlungen entsprechend modifizieren.

3.4. Prüfungsdurchführung

3.4.1. Prüfung der Ausgestaltung und Aktualität der CMS-Beschreibung

54 Der CMS-Prüfer hat die Ausgestaltung und Aktualität der CMS-Beschreibung zu beurteilen. Hinsichtlich der Ausgestaltung der CMS-Beschreibung hat der CMS-Prüfer zu beurteilen, ob die von den gesetzlichen Vertretern aufgestellte CMS-Beschreibung die Regelungen zum Aufbau und zur Funktionsweise des CMS vollständig und richtig sowie in einer für die Nutzer verständlichen Art und Weise darstellt (vgl. Tz. A14). Hierzu zählen auch die bei der Ausgestaltung des CMS angewandten CMS-Grundsätze. Die Prüfung der Vollständigkeit umfasst auch, ob die Darstellungen der gesetzlichen Vertreter zu den Regelungen des CMS auf sämtliche der in Tz. 27 genannten Grundelemente eines CMS eingehen.

55 Hinsichtlich der Aktualität der CMS-Beschreibung ist festzustellen, ob die CMS-Beschreibung dem zu prüfenden Stand des CMS entspricht oder ob zwischenzeitlich Änderungen vorgenommen wurden, die aus Sicht des CMS-Prüfers als wesentlich zu erachten sind. Soweit dies der Fall ist, hat der CMS-Prüfer die gesetzlichen Vertreter aufzufordern, die CMS-Beschreibung entsprechend anzupassen.

56 Im Falle einer Wirksamkeitsprüfung hat der CMS-Prüfer auch zu beurteilen, ob die CMS-Beschreibung auf wesentliche Veränderungen im CMS, bezogen auf den Betrachtungszeitraum, gesondert eingeht.

3.4.2. Prüfung der in der CMS-Beschreibung enthaltenen Darstellungen zur Angemessenheit und Wirksamkeit des CMS

3.4.2.1. Angemessenheit der in der CMS-Beschreibung dargestellten Regelungen des CMS

57 Der CMS-Prüfer hat die Ergebnisse seiner Risikobeurteilungen bei den weiteren Prüfungshandlungen zu berücksichtigen. Wenn dem CMS-Prüfer bereits anlässlich der Prüfungshandlungen zur Gewinnung eines Verständnisses von dem zu prüfenden CMS und zur CMS-Beschreibung wesentliche falsche Darstellungen bzw. Mängel bekannt werden, kann er zu dem Ergebnis gelangen, dass das dargestellte CMS nicht angemessen ausgestaltet ist. In diesem Fall erübrigen sich weitere Prüfungshandlungen zur Angemessenheit und Wirksamkeit des CMS.

58 Im Rahmen der Prüfung der Angemessenheit des CMS hat der CMS-Prüfer zu beurteilen, ob die in der CMS-Beschreibung des Unternehmens dargestellten Regelungen des CMS so ausgestaltet und implementiert sind, dass sie geeignet sind, mit hinreichender Sicherheit sowohl

Risiken für wesentliche Regelverstöße rechtzeitig zu erkennen als auch solche Regelverstöße zu verhindern

59 Der CMS-Prüfer hat durch die Kombination von Befragungen mit anderen Prüfungshandlungen, einschließlich Beobachtung sowie Einsichtnahme in Aufzeichnungen und Dokumente, festzustellen, ob das CMS wie beschrieben zu einem bestimmten Zeitpunkt eingerichtet (implementiert) ist (vgl. Tz. A49 ff.).

3.4.2.2. Wirksamkeit der in der CMS-Beschreibung dargestellten Regelungen des CMS

60 Die Prüfung der Wirksamkeit der in der CMS-Beschreibung dargestellten Regelungen des CMS zielt zusätzlich auf die Beurteilung ab, ob die in der CMS-Beschreibung dargestellten Regelungen innerhalb des gesamten zu prüfenden Zeitraums wie vorgesehen eingehalten wurden (vgl. Tz. A51 ff.).

61 Die Beurteilung der Kontinuität der Beachtung der in der CMS-Beschreibung dargestellten Regelungen erfordert es, dass die Prüfung der Wirksamkeit einen angemessenen Zeitraum abdeckt, i.d.R. mindestens ein halbes Geschäftsjahr.

62 Sofern Prüfungshandlungen zur Beurteilung der Wirksamkeit der in der CMS-Beschreibung dargestellten Regelungen zu einem vorgezogenen Zeitpunkt durchgeführt werden, sind weitere Prüfungsnachweise zur Beurteilung der Wirksamkeit bis zum Ende des zu prüfenden Zeitraums einzuholen.

3.4.3. Weitere Prüfungshandlungen

3.4.3.1. Festgestellte Regelverstöße

63 Stellt der CMS-Prüfer anlässlich seiner Prüfungstätigkeit Regelverstöße fest oder liegen ihm entsprechende Anhaltspunkte vor, hat er die Mitglieder des Managements auf einer angemessenen Zuständigkeitsebene und ggf. die für die Überwachung Verantwortlichen in angemessener Zeit darüber zu informieren, sofern diese nicht bereits nachweisbar über die konkreten Fälle auf andere Art und Weise informiert wurden. Bei festgestellten Regelverstößen liegt es in der Verantwortung der gesetzlichen Vertreter zu untersuchen, welche Umstände zu dem Regelverstoß geführt haben und warum das CMS den Regelverstoß nicht verhindert hat. Der CMS-Prüfer hat den informierten Personenkreis darauf hinzuweisen, dass die CMS-Prüfung nicht darauf ausgerichtet ist, einzelne Regelverstöße aufzudecken.

64 Der CMS-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 CMS-Prüfer nicht davon ausgehen, dass es sich bei dem Regelverstoß um einen einmaligen Vorgang handelt (vgl. Tz. A61).

3.4.3.2. Nutzung der Arbeit von Sachverständigen des CMS-Prüfers

65 Wenn die Beurteilung bedeutsamer Sachverhalte besondere Sachkenntnisse erfordert, um ausreichende geeignete Prüfungsnachweise zu erlangen, hat der CMS-Prüfer zu entscheiden, ob Sachverständige hinzuzuziehen sind (vgl. Tz. A62).

66 Eingesetzte interne Sachverständige des CMS-Prüfers müssen dem Qualitätssicherungssystem der WP-Praxis unterliegen. Der CMS-Prüfer hat die internen Sachverständigen angemessen anzuleiten, sie zu beaufsichtigen und die Dokumentation der Tätigkeit der Sachverständigen durchzusehen.

67 Wenn die Arbeiten eines Sachverständigen des CMS-Prüfers zu nutzen sind, hat der CMS-Prüfer

- zu beurteilen, ob der Sachverständige über die Kompetenz, die Fähigkeiten und die Objektivität verfügt, die für die Zwecke der CMS-Prüfung notwendig sind. Die Beurteilung der Objektivität des externen Sachverständigen umfasst u.a. eine Befragung zu möglichen Interessen und Beziehungen, die eine Gefährdung der Objektivität des Sachverständigen hervorrufen können (vgl. Tz. A63),
- ein ausreichendes Verständnis von dem Fachgebiet des Sachverständigen zu erlangen,
- mit dem Sachverständigen Art, Umfang und Ziele der Arbeit für die Zwecke der CMS-Prüfung zu vereinbaren und
- die Angemessenheit der Arbeit des Sachverständigen für die Zwecke der Prüfung des CMS zu beurteilen (vgl. Tz. A64 f.).

3.4.3.3. Nutzung der Arbeit anderer Prüfer

68 Plant der CMS-Prüfer die Nutzung der Arbeit eines anderen Prüfers, hat er zu beurteilen, ob dessen Arbeit für seine Zwecke geeignet ist (vgl. Tz. A66).

3.4.3.4. Nutzung der Arbeit von Sachverständigen der gesetzlichen Vertreter

69 Sollen Informationen, die unter Nutzung der Tätigkeit eines Sachverständigen der gesetzlichen Vertreter erstellt wurden, als Prüfungsnachweise verwendet werden, muss der CMS-Prüfer, soweit notwendig, unter Berücksichtigung der Bedeutung der Tätigkeit des Sachverständigen für die Zwecke des CMS-Prüfers

- die Kompetenz, Fähigkeiten und Objektivität des Sachverständigen beurteilen,
- ein ausreichendes Verständnis von der Tätigkeit des Sachverständigen gewinnen und
- die Angemessenheit der Tätigkeit des Sachverständigen als Prüfungsnachweis beurteilen (vgl. Tz. A66).

3.4.3.5. Nutzung der Arbeit der Internen Revision

70 Plant der CMS-Prüfer, Arbeiten der Internen Revision zu nutzen, hat er zu beurteilen,

- inwieweit die organisatorische Stellung und die Arbeitsweise die notwendige Objektivität der Internen Revisoren unterstützt,

- ob die notwendige fachliche Kompetenz der Internen Revision vorhanden ist,
- ob die Arbeiten der Internen Revision mit einer systematischen und strukturierten Vorgehensweise (einschließlich qualitätssichernder Maßnahmen) durchgeführt werden und
- ob die Arbeiten der Internen Revision für Zwecke der Prüfung des CMS angemessen sind (vgl. Tz. A66 f.).

71 Für die Frage, inwieweit sich die Arbeiten der Internen Revision auf die Art, den Umfang und den Zeitpunkt der eigenen Prüfungshandlungen auswirken, hat der CMS-Prüfer Folgendes zu berücksichtigen:

- Art und Umfang der Revisionstätigkeiten (sowohl durchgeführte als auch noch durchzuführende)
- Relevanz der Revisionstätigkeit für die eigene Prüfung
- Nachvollziehbarkeit der Revisionsergebnisse
- Art, Umfang und Ergebnisse einer Prüfung nach *IDW PS 983* oder DIIR Standard Nr. 3.

3.4.3.6. Ereignisse nach dem Beurteilungszeitpunkt bzw. -zeitraum

72 Der CMS-Prüfer hat die Auswirkungen von Ereignissen nach dem Zeitpunkt bzw. Zeitraum, auf den sich die Darstellungen in der CMS-Beschreibung beziehen, bis zum Datum des CMS-Prüfungsberichts zu würdigen (vgl. Tz. A68).

73 Der CMS-Prüfer ist nicht verpflichtet, Prüfungshandlungen nach dem Datum des CMS-Prüfungsberichts durchzuführen oder Prüfungshandlungen durchzuführen, um Ereignisse festzustellen, die nicht den Prüfungszeitraum betreffen.

74 Falls dem CMS-Prüfer nach dem Datum des CMS-Prüfungsberichts bis zur Auslieferung des Berichts Sachverhalte bekannt werden, die auf Mängel oder bedeutsame zwischenzeitliche Änderungen im CMS hindeuten, auf die in der CMS-Beschreibung nicht eingegangen wird, hat er auf eine Änderung der CMS-Beschreibung durch das Unternehmen hinzuwirken. Unterbleibt eine Änderung, hat er zu untersuchen, ob weitere Prüfungshandlungen vorzunehmen sind, um festzustellen, ob die betreffenden Sachverhalte eine Auswirkung auf sein Prüfungsurteil haben (vgl. Tz. A69).

75 Werden dem CMS-Prüfer nach dem Datum des CMS-Prüfungsberichts Sachverhalte bekannt, die dazu führen, dass das Prüfungsurteil in der erteilten Form nicht hätte abgegeben werden dürfen, hat er angemessene Maßnahmen zu ergreifen, damit die Nutzer des CMS-Berichts hiervon Kenntnis erlangen. Die Einholung rechtlichen Rats kann angezeigt sein.

3.4.3.7. Sonstige Informationen in der CMS-Beschreibung

76 Enthält die CMS-Beschreibung sonstige Informationen, die nicht Gegenstand der Auftragsvereinbarung sind (vgl. Tz. A36), hat der CMS-Prüfer darauf hinzuwirken, dass die gesetzlichen Vertreter diese sonstigen Informationen in der CMS-Beschreibung unterlassen oder sie eindeutig von den prüfungsrelevanten Darstellungen der CMS-Beschreibung abgrenzen (vgl. Tz. A70).

77 Es liegt im Ermessen des CMS-Prüfers, ob die sonstigen Informationen in die Prüfung einbezogen werden.

Der CMS-Prüfer hat die nicht in die inhaltliche Prüfung einbezogenen sonstigen Informationen im CMS-Prüfungsbericht zu benennen und darauf hinzuweisen, dass sie nicht in die inhaltliche Prüfung einbezogen wurden und sich daher das Prüfungsurteil nicht darauf erstreckt. Nicht in die inhaltliche Prüfung einbezogene sonstige Informationen hat der CMS-Prüfer jedoch zu lesen, um etwaige bestehende wesentliche Unstimmigkeiten gegenüber den geprüften Darstellungen in der CMS-Beschreibung festzustellen.

78 Falls der CMS-Prüfer beim Lesen der sonstigen Informationen

- eine wesentliche Unstimmigkeit zwischen den sonstigen Informationen und den geprüften Darstellungen in der CMS-Beschreibung oder den Aussagen im CMS-Prüfungsbericht feststellt oder
- wesentliche Fehler in den sonstigen Informationen feststellt, die nicht mit den geprüften Darstellungen in der CMS-Beschreibung und den Aussagen im CMS-Prüfungsbericht zusammenhängen,

hat er den Sachverhalt mit den gesetzlichen Vertretern zu erörtern und, sofern angebracht, weitere angemessene Maßnahmen zu ergreifen (vgl. Tz. A70).

79 Hat der CMS-Prüfer festgestellt, dass die Klarheit und Übersichtlichkeit der CMS-Beschreibung durch die sonstigen Informationen, die nicht Gegenstand der inhaltlichen Prüfung sind, wesentlich beeinträchtigt sind, hat er das Prüfungsurteil einzuschränken oder zu versagen.

3.4.3.8. Schriftliche Erklärungen

80 Der CMS-Prüfer hat vor Abschluss der Prüfung von den gesetzlichen Vertretern eine Vollständigkeitserklärung[15] einzuholen, in der bestätigt wird, dass die CMS-Beschreibung auf der Grundlage der angewandten CMS-Grundsätze des CMS vollständig und richtig ist und dem Prüfer, wie in den Auftragsbedingungen vereinbart, alle relevanten Erklärungen und Nachweise zur Angemessenheit, Implementierung und sofern einschlägig Wirksamkeit des CMS erteilt worden sind. Dazu gehört auch die Zusicherung, dass die gesetzlichen Vertreter dem CMS-Prüfer vollständig die folgenden ihnen bekannten Aspekte mitgeteilt haben:

- Mängel in Bezug auf die Angemessenheit oder Wirksamkeit des CMS
- Fälle, in denen die Regelungen des CMS nicht, wie in der CMS-Beschreibung dargestellt, implementiert oder durchgeführt wurden
- geplante bedeutsame Änderungen im CMS
- Ereignisse, die nach dem Prüfungszeitraum, aber vor dem Datum des CMS-Prüfungsberichts eingetreten sind und eine erhebliche Auswirkung auf die Darstellungen in der CMS-Beschreibung haben können (vgl. Tz. A72).

81 Die Vollständigkeitserklärung muss zeitnah zum Datum des CMS-Prüfungsberichts, darf aber nicht nach diesem datiert werden.

[15] Muster der Vollständigkeitserklärungen für die Prüfung von CMS sind bei der IDW Verlag GmbH, Postfach 32 05 80, 40420 Düsseldorf erhältlich.

82 Der CMS-Prüfer hat über die Einholung der Vollständigkeitserklärung hinaus weitere schriftliche Erklärungen zu erlangen, um andere für die CMS-Beschreibung relevante Prüfungsnachweise zu stützen, sofern er dies für erforderlich hält.

83 Sofern sich einzelne Aspekte der Vollständigkeitserklärung oder weiterer schriftlicher Erklärungen auf Sachverhalte beziehen, die wesentlich für die Darstellungen in der CMS-Beschreibung sind, muss der CMS-Prüfer

- die Begründetheit dieser Erklärung(en) und deren Konsistenz zu anderen erlangten Nachweisen, einschließlich anderer mündlicher oder schriftlicher Erklärungen der gesetzlichen Vertreter, beurteilen und
- abwägen, ob zu erwarten ist, dass die Personen, welche die schriftlichen Erklärungen abgeben, in Bezug auf die betreffenden Sachverhalte ausreichend informiert sind.

84 Weigern sich die gesetzlichen Vertreter, eine Vollständigkeitserklärung abzugeben, oder bestehen begründete Zweifel in Bezug auf die Kompetenz oder die Integrität der Personen, welche die Vollständigkeitserklärung abgeben, bzw. bestehen andere begründete Zweifel, dass die erteilte Erklärung verlässlich ist, ist darin ein Prüfungshemmnis zu sehen. In diesem Fall hat der CMS-Prüfer im Prüfungsbericht zu erklären, dass ein Prüfungsurteil nicht abgegeben wird.

Beziehen sich die Zweifel auf andere vom CMS-Prüfer angeforderte schriftliche Erklärungen, hat der CMS-Prüfer den Sachverhalt mit den Verantwortlichen zu erörtern, die Auswirkungen auf die Verlässlichkeit der bereits eingeholten Prüfungsnachweise zu würdigen und, sofern angebracht, weitere Maßnahmen zu ergreifen, einschließlich der Feststellung möglicher Auswirkungen auf das Prüfungsurteil.

3.4.4. Auswertung der Prüfungsfeststellungen und Bildung des Prüfungsurteils

85 Der CMS-Prüfer muss würdigen, ob ausreichende geeignete Prüfungsnachweise als Grundlage für die Beurteilung der Darstellungen in der CMS-Beschreibung über die Angemessenheit, Implementierung bzw. Wirksamkeit des CMS erlangt wurden. Ist dies der Fall, hat der CMS-Prüfer die Prüfungsfeststellungen auszuwerten und auf dieser Grundlage ein Prüfungsurteil zu treffen. Anderenfalls hat der CMS-Prüfer weitere Prüfungsnachweise einzuholen.

86 Bei der Bildung des Prüfungsurteils hat der CMS-Prüfer zu beurteilen, ob nicht korrigierte falsche Darstellungen in der CMS-Beschreibung bzw. festgestellte Mängel in dem in der CMS-Beschreibung dargestellten CMS einzeln oder in der Summe wesentlich sind. Hierbei hat der CMS-Prüfer alle relevanten Prüfungsnachweise zu berücksichtigen, unabhängig davon, ob sie dem Anschein nach die Darstellungen in der CMS-Beschreibung stützen oder ihnen widersprechen (vgl. Tz. A73).

87 Enthält die CMS-Beschreibung keine wesentlichen falschen Darstellungen, hat der CMS-Prüfer ein uneingeschränktes Prüfungsurteil abzugeben. Liegen wesentliche falsche Darstellungen vor, ist das Prüfungsurteil einzuschränken oder zu versagen.

88 Das Prüfungsurteil ist wegen einer falschen Darstellung in der CMS-Beschreibung einzuschränken, wenn die falsche Darstellung zwar wesentlich, aber nicht umfassend ist. Sind die falschen Darstellungen so bedeutend oder so zahlreich, dass nach der pflichtgemäßen Beurteilung des CMS-Prüfers keine Einschränkung in Bezug auf die geprüfte CMS-Beschreibung

bzw. auf die Angemessenheit und sofern einschlägig Wirksamkeit des darin dargestellten CMS mehr in Frage kommt, z.B. weil aufgrund von umfassenden Mängeln bei der Konzeption des CMS oder einer ungünstigen Compliance-Kultur die Regelungen des CMS insgesamt als nicht angemessen anzusehen sind, ist das Prüfungsurteil zu versagen.

89 Ist der CMS-Prüfer nicht in der Lage, ausreichende geeignete Prüfungsnachweise zu erlangen, liegt ein Prüfungshemmnis vor. In diesem Fall ist das Prüfungsurteil einzuschränken, wenn die Auswirkungen des Prüfungshemmnisses zwar die Beurteilung eines wesentlichen Teils der Darstellungen in der CMS-Beschreibung ausschließen, eine Beurteilung insgesamt aber noch möglich ist. Kann aufgrund von Prüfungshemmnissen auch nach Ausschöpfung der prüferischen Möglichkeiten ein Urteil nicht abgegeben werden, hat der CMS-Prüfer in der Berichterstattung zu erklären, dass ein Prüfungsurteil nicht abgegeben wird.

90 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, hat der CMS-Prüfer zunächst auf eine entsprechende Änderung der CMS-Beschreibung hinzuwirken. Unterbleibt eine Änderung, hat er abzuwägen, ob das Prüfungsurteil einzuschränken oder zu versagen ist. Wenn sich im Verlauf der Prüfung herausstellt, dass die zu prüfenden Teilbereiche von den gesetzlichen Vertretern irreführend festgelegt wurden oder die angewandten CMS-Grundsätze nicht geeignet sind, hat der CMS-Prüfer das Prüfungsurteil zu versagen.

91 Einschränkungen, Versagungen oder die Erklärung der Nichtabgabe des Prüfungsurteils sind klar durch die Verwendung des Begriffs „Einschränkung“ bzw. „Versagung“ oder „Nichtabgabe“ zu kennzeichnen. Die Gründe für die Einschränkung bzw. Versagung oder die Nichtabgabe des Prüfungsurteils sind vollständig und eindeutig im CMS-Prüfungsbericht darzustellen.

92 Hält der CMS-Prüfer es für notwendig, die Berichtsadressaten auf einen in der CMS-Beschreibung enthaltenen Sachverhalt aufmerksam zu machen, der nach der Beurteilung des CMS-Prüfers grundlegend für das Verständnis der CMS-Beschreibung durch die Nutzer des CMS-Prüfungsberichts ist, muss der CMS-Prüfer einen Hinweis zur Hervorhebung des Sachverhalts in den CMS-Prüfungsbericht aufnehmen. Dieser Hinweis darf sich nur auf in der CMS-Beschreibung angegebene Informationen beziehen.

93 Darüber hinaus hat der CMS-Prüfer auf sonstige Sachverhalte hinzuweisen, auch wenn diese nicht in der CMS-Beschreibung dargestellt sind, wenn dies nach der Beurteilung des CMS-Prüfers für die Nutzer des CMS-Prüfungsberichts zum Verständnis des Prüfungsauftrags, der Verantwortung des CMS-Prüfers oder zum Verständnis des CMS-Prüfungsberichts erforderlich ist. Ein Hinweis auf sonstige Sachverhalte ist – ebenso wie ein Hinweis zur Hervorhebung eines Sachverhalts nach Tz. 92 – klar zu kennzeichnen und es ist klarzustellen, dass das Prüfungsurteil im Hinblick auf den entsprechenden Sachverhalt nicht eingeschränkt oder versagt wird.

3.4.5. Dokumentation

94 Der CMS-Prüfer hat die zur Stützung seines Prüfungsurteils dienenden Prüfungsnachweise in angemessener Zeit in den Arbeitspapieren zu dokumentieren.

95 Form und Inhalt der Dokumentation stehen im pflichtgemäßen Ermessen des CMS-Prüfers. Die Arbeitspapiere sind so anzulegen, dass sich ein erfahrener Wirtschaftsprüfer, der nicht mit der Prüfung befasst war, in angemessener Zeit ein Bild über die Abwicklung und Ergebnisse der Prüfung machen kann.

96 Anhand der Dokumentation muss ein erfahrener Wirtschaftsprüfer folgende Punkte in angemessener Zeit nachvollziehen können (vgl. Tz. A74):

- Einhaltung der Berufspflichten (einschließlich des Grundsatzes der Unabhängigkeit, möglicher Unabhängigkeitsgefährdungen und deren Lösung)
- Art, zeitliche Einteilung und Umfang der durchgeführten Prüfungshandlungen
- die Ergebnisse der Prüfungshandlungen und die erlangten Prüfungsnachweise und
- bedeutsame Sachverhalte, die während der Prüfung aufgetreten sind, die diesbezüglichen Schlussfolgerungen und die bei der Erlangung dieser Schlussfolgerungen getroffenen bedeutsamen Beurteilungen.

97 Im Rahmen der Dokumentation von Art, Umfang und Zeitpunkten der Prüfungshandlungen hat der CMS-Prüfer aufzuzeichnen,

- welche Prüfungsnachweise zur Angemessenheit und Wirksamkeit des CMS erlangt wurden nebst deren eindeutiger Bezeichnung,
- von wem die Prüfungshandlungen durchgeführt und wann sie abgeschlossen wurden,
- von wem und wann die Prüfungshandlungen kontrolliert wurden sowie den Inhalt dieser Überprüfung.

98 Soweit der CMS-Prüfer bestimmte Arbeiten der Internen Revision oder von Sachverständigen nutzt, hat er dies zu dokumentieren. Hiervon umfasst ist die Dokumentation seiner Beurteilungsergebnisse sowie seiner in diesem Zusammenhang durchgeführten Prüfungshandlungen.

99 Erhält der CMS-Prüfer Informationen, die einer zuvor erfolgten abschließenden Beurteilung eines bedeutsamen Prüfungssachverhalts entgegenstehen, hat er die in diesem Zusammenhang ergriffenen Maßnahmen (z.B. die Durchführung zusätzlicher Prüfungshandlungen) zu dokumentieren.

100 Der Abschluss der Auftragsdokumentation hat innerhalb eines angemessenen Zeitraums nach dem Datum des CMS-Prüfungsberichts zu erfolgen. Die Löschung bzw. das Entfernen von Dokumentationen ist nach der abschließenden Zusammenstellung der Arbeitspapiere und finalen Auftragsdokumentation vor dem Ablauf der Aufbewahrungsfrist unzulässig.

101 Für den Fall, dass der CMS-Prüfer es für notwendig erachtet, die Auftragsdokumentation nach der abschließenden Zusammenstellung zu ändern oder zu ergänzen, und dies keine Auswirkungen auf den CMS-Prüfungsbericht hat, ist Folgendes zu dokumentieren:

- Die Gründe für die Änderungen bzw. Ergänzungen und
- von wem sie wann durchgeführt und
- von wem sie wann durchgesehen wurden

3.4.6. Berichterstattung des CMS-Prüfers

3.4.6.1. CMS-Prüfungsbericht

102 Der CMS-Prüfer hat einen schriftlichen CMS-Prüfungsbericht zu verfassen, der ein Prüfungsurteil über die in der CMS-Beschreibung gegebenen Darstellungen enthält bzw. erforderlichenfalls eine Erklärung enthält, dass ein Prüfungsurteil nicht abgegeben werden kann.

103 Im CMS-Prüfungsbericht ist das Prüfungsurteil von anderen Informationen und Erläuterungen (z.B. Hervorhebungen und Hinweisen (vgl. Tz. 92 f.) oder von Feststellungen und Empfehlungen zum CMS, die keinen Einfluss auf das Urteil haben) klar zu trennen.

104 Der CMS-Prüfungsbericht muss folgende Bestandteile enthalten:

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

b) Adressaten des CMS-Prüfungsberichts

c) Prüfungsauftrag

d) Beschreibung (Identifizierung) des zu prüfenden CMS

e) Angabe der oder Bezugnahme auf die vom Unternehmen angewandten CMS-Grundsätze, anhand derer die Angemessenheit und Wirksamkeit des abgegrenzten CMS-Teilbereichs beurteilt wird, so dass die beabsichtigten Nutzer die Grundlage für die Schlussfolgerungen des Prüfers verstehen können. Der CMS-Prüfungsbericht nennt die anwendbaren CMS-Grundsätze oder verweist auf sie, wenn sie in der CMS-Beschreibung enthalten sind oder wenn sie anderweitig aus einer allgemein zugänglichen Quelle verfügbar sind.

f) Gegenstand, Art und Umfang der Prüfung einschließlich einer zusammenfassenden Beschreibung der durchgeführten Prüfungshandlungen (Prüfungshandlungen zur Risikobeurteilung, Angemessenheits- und Wirksamkeitsprüfung sowie der weiteren Prüfungshandlungen) einschließlich der Klarstellung, dass es sich um einen Auftrag zur Erlangung hinreichender Sicherheit über die in der CMS-Beschreibung enthaltenen Darstellungen zu dem CMS handelt

g) Beschreibung der Verantwortlichkeiten der gesetzlichen Vertreter und des CMS-Prüfers

h) Aussage, dass die Prüfung in Übereinstimmung mit diesem *IDW Prüfungsstandard* durchgeführt wurde; der CMS-Prüfer darf nicht die Einhaltung dieses *IDW Prüfungsstandards* erklären oder suggerieren, wenn er nicht sämtliche einschlägigen Anforderungen dieses *IDW Prüfungsstandards* beachtet hat

i) Aussage, dass bei der Prüfung die Berufspflichten der WPO und der Berufssatzung WP/vBP, einschließlich der Anforderungen an die Unabhängigkeit, eingehalten werden und dass die WP-Praxis die Anforderungen an die Qualitätssicherung anwendet

j) Feststellungen zum CMS und ggf. Empfehlungen

k) Falls relevant:

- Beschreibung von bedeutenden Schwierigkeiten bei der Beurteilung des Prüfungsgegenstands
- Aussage, dass der Auftrag für einen bestimmten Zweck bzw. Adressatenkreis durchgeführt wurde und deshalb die Verwendung der Ergebnisse für andere Zwecke ausgeschlossen ist

- ggf. Hinweis auf nicht in die inhaltliche Prüfung einbezogene und vom Unternehmen abgegrenzte sonstige Informationen in der CMS-Beschreibung (vgl. Tz. 76 ff.)

l) Zusammenfassendes Prüfungsurteil (vgl. Tz. 15 ff.)

m) Eine Aussage über die inhärenten Grenzen des CMS und zum Risiko, die Feststellungen zum CMS auf die Zukunft zu übertragen

n) Datum des CMS-Prüfungsberichts: Das Datum darf nicht vor dem Datum liegen, an dem der CMS-Prüfer ausreichende und angemessene Nachweise als Grundlage für das Prüfungsurteil über das CMS erlangt hat und die Vollständigkeitserklärung der gesetzlichen Vertreter vorliegt.

o) Name und Ort des CMS-Prüfers.

p) Unterschrift des CMS-Prüfers.

105 Da die freiwillige Prüfung von CMS keine Vorbehaltsaufgabe i.S. des § 48 Abs. 1 Satz 1 WPO ist, besteht keine Pflicht zur Führung des Siegels.

106 Wenn der CMS-Prüfer auf die Arbeit eines Sachverständigen des CMS-Prüfers (vgl. Tz. 65 ff.) Bezug nimmt, darf nicht der Eindruck entstehen, dass die Verantwortung des CMS-Prüfers für das Prüfungsurteil durch diese Bezugnahme verringert wird.

107 Die CMS-Beschreibung der gesetzlichen Vertreter ist dem CMS-Prüfungsbericht als Anlage beizufügen.

108 Beispiele für CMS-Prüfungsberichte finden sich in Anlage 3 zu diesem *IDW Prüfungsstandard*. Der CMS-Prüfer kann für den Fall einer Wirksamkeitsprüfung mit dem Auftraggeber vereinbaren, eine Kurzfassung des CMS-Prüfungsberichts zu erstellen. Die Erstellung eines solchen Kurzberichts kommt nur bei einer vollumfänglichen Prüfung der Wirksamkeit der in der CMS-Beschreibung dargestellten Regelungen des Unternehmens in Betracht. Die Kurzfassung muss neben einer klarstellenden Überschrift die in Tz. 104 genannten Mindestbestandteile – mit Ausnahme der ggf. nicht oder nicht vollständig aufzuführenden Feststellungen und Empfehlungen – enthalten. In der Kurzfassung ist zudem auf den vollständigen Prüfungsbericht zu verweisen. Ein **Formulierungsbeispiel für einen Kurzbericht** findet sich in **Anlage 3.4** zu diesem *IDW Prüfungsstandard*.

3.4.6.2. Weitere Berichtspflichten

109 Wenn nach der Einschätzung des CMS-Prüfers bestimmte Prüfungsfeststellungen eine unmittelbare Reaktion des Unternehmens erfordern, ist darüber vorab gegenüber dem Auftraggeber zu berichten.

110 Der CMS-Prüfer muss feststellen, ob ggf. weitere Berichtspflichten bestehen, z.B. gegenüber den für die Überwachung des Unternehmens Verantwortlichen. Im Falle einer Berichtspflicht ist diese im CMS-Prüfungsbericht oder in sonstiger geeigneter Weise zu erfüllen (vgl. Tz. A76).

4. Anwendungshinweise und sonstige Erläuterungen

Vorbemerkungen [Tz. 1 ff.]

A1 Die Pflicht zur Einrichtung eines internen Kontrollsystems und Risikomanagementsystems (vgl. Tz. 2) kann für die Vorstandsmitglieder nichtbörsennotierter Unternehmen weiterhin aus der sie treffenden Sorgfaltspflicht nach § 93 Abs. 1 AktG folgen.[16]

A2 Die in § 107 Abs. 3 Satz 2 AktG genannten Bereiche (vgl. Tz. 4) sind als eine Konkretisierung der allgemeinen Überwachungsaufgabe des Aufsichtsrats aus § 111 Abs. 1 AktG anzusehen. Der Aufsichtsrat hat die genannten Aufgaben selbst wahrzunehmen, wenn er keinen Prüfungsausschuss einrichtet.[17]

Die Vorschriften des § 111 AktG finden nicht nur auf die Aktiengesellschaft und die Kommanditgesellschaft auf Aktien (KGaA) (§ 278 Abs. 3 AktG), sondern nach § 25 Abs. 1 Satz 1 Nr. 2 MitbestG, § 3 Abs. 2 MontanMitbestG, § 3 Abs. 1 MitbestErgG, § 1 Abs. 1 Nr. 3 DrittelbG, § 24 Abs. 2 Satz 2 MgVG auch auf die mitbestimmte GmbH Anwendung. Auf die mitbestimmungsfreie GmbH findet § 111 AktG nach § 52 Abs. 1 GmbHG nur insoweit Anwendung, als im Gesellschaftsvertrag nicht etwas anderes bestimmt ist.

A3 Die durch den Aufsichtsrat bzw. den Prüfungsausschuss zu überwachenden Corporate Governance Systeme

- Internes Kontrollsystem (IKS),
- Risikomanagementsystem (RMS),
- Internes Revisionssystem (IRS) und
- Compliance Management System (CMS)

werden im Gesetz nicht näher beschrieben und auch in der Literatur nicht einheitlich definiert bzw. zueinander abgegrenzt. Zur Systematik des Zusammenspiels dieser Corporate Governance Systeme lehnt sich dieser *IDW Prüfungsstandard* an das COSO-Rahmenwerk zum unternehmensweiten Risikomanagement[18] an.

A4 Sollte es an den in Tz. A3 genannten wirksamen Systemen fehlen, obliegt dem Aufsichtsrat bzw. dem von ihm eingerichteten Prüfungsausschuss die Prüfung, ob der Verzicht zur Einrichtung entsprechender Systeme mit den Organisations- und Sorgfaltspflichten des Vorstands nach § 93 Abs. 1 Satz 1 AktG in Einklang steht.

A5 Diese Systematisierung verschiedener (Teil-)Systeme der Corporate Governance setzt keine separate Aufbau- oder Ablauforganisation der genannten Systeme im Unternehmen voraus. In Abhängigkeit von Art, Umfang und Komplexität der Geschäftstätigkeit werden in der Praxis häufig integrierte Systeme entwickelt. Darüber hinaus wird in der Praxis auch das Three-Lines-

---

[16] Vgl. BT-Drucks. 19/26966, S. 115.

[17] Vgl. BT-Drucks. 16/10067, S. 102.

[18] Unternehmensweites Risikomanagement – Übergreifendes Rahmenwerk (COSO ERM): https://www.coso.org/Pages/erm.aspx (letzter Aufruf: 19.11.2021).

Modell[19] verwendet, um die Rollen und Verantwortlichkeiten sowie die Abgrenzung der Funktionen der jeweiligen Corporate Governance Systeme untereinander zu beschreiben.

A6 Die Prüfung des CMS i.S. dieses *IDW Prüfungsstandards* umfasst stets sämtliche Grundelemente (vgl. Tz. 7). Eine isolierte Prüfung in Bezug auf einzelne Grundelemente (z.B. nur die Prüfung des Grundelements Compliance-Programm, ohne zu berücksichtigen, wie das Unternehmen die Compliance-Ziele festlegt oder Compliance-Risiken identifiziert), liegt nicht im Anwendungsbereich dieses *IDW Prüfungsstandards*.

A7 Folgende abgegrenzte Teilbereiche können z.B. Gegenstand einer CMS-Prüfung sein (vgl. Tz. 13d)):

- Rechtsgebiete:
  - Wettbewerbs- und Kartellrecht
  - Antikorruptionsrecht (z.B. § 298 ff. StGB oder Foreign Corrupt Practices Act – FCPA, UK-Bribery Act)
  - Steuerrecht (z.B. Umsatzsteuer, Ertragsteuern, Lohnsteuer)
  - Geldwäschegesetz
  - Datenschutz- und Datensicherheitsvorschriften
  - Börsenrecht (z.B. Vorschriften zum Insiderhandel oder zu Ad-hoc-Meldepflichten)
  - Vorschriften zur Unternehmensführung und -überwachung (z.B. nach dem Deutschen Corporate Governance Kodex)
  - Umweltrecht
  - Außenwirtschaftsrecht und Exportkontrolle
  - Arbeitsrecht und Persönlichkeitsrechte (z.B. Allgemeines Gleichstellungsgesetz)
  - Arbeitssicherheitsrecht
  - Zollrecht
  - Patent- und Markenrecht (Intellectual Property)
  - Produkthaftungsrecht
- Organisation der Einhaltung von Selbstverpflichtungen.

Darüber hinaus kommt zusätzlich eine Abgrenzung nach Organisationseinheiten des Unternehmens (z.B. Divisionen vgl. auch Tz. A16) oder Regionen (z.B. nach Ländern) in Frage.

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.

[19] Das Three-Lines Modell wurde vom Dachverband der europäischen Revisionsinstitute (ECIIA) als Leitfaden zur Umsetzung der Abschlussprüferrichtlinie entwickelt, um die unterschiedlichen Rollen zur internen Steuerung und deren Zusammenspiel zu erklären und darzustellen. Es wurde mit Herausgabe eines umfangreichen Positionspapiers durch das Institute of Internal Auditors im Januar 2013 weltweit in seiner Bedeutung hervorgehoben und in 2020 überarbeitet (– https://na.theiia.org/about-ia/PublicDocuments/Three-Lines-Model-Updated.pdf (letzter Aufruf: 19.11.2021).

Definitionen [Tz. 13 ff.]

A8 Interne Richtlinien des Unternehmens (Tz. 13a)) können auch von Dritten entwickelte Prinzipien oder Konventionen sein, zu deren Einhaltung sich das Unternehmen selbst verpflichtet hat.

A9 Die in den Grundelementen des CMS zum Ausdruck kommenden Regelungen bilden in ihrer Gesamtheit das Compliance Management System (vgl. Tz. 13b)).

A10 Der Begriff Compliance Management System (vgl. Tz. 13b)) ist unabhängig von der Bezeichnung einzelner Abteilungen und Funktionen im Unternehmen zu verstehen.

A11 Das CMS ist integraler Bestandteil der Corporate Governance des Unternehmens. Die Notwendigkeit zur Einrichtung einer eigenständigen Aufbau- und Ablauforganisation für das CMS ist abhängig von Art, Umfang und Komplexität der Geschäftstätigkeit des Unternehmens.

A12 Im Rahmen der Ausgestaltung des CMS entscheiden die gesetzlichen Vertreter u.a., welche CMS-Grundsätze (vgl. Tz. 13e)) angewendet werden sollen. Hierbei kommen die in Anlage 1 genannten allgemein anerkannten Rahmenkonzepte, andere geeignete Rahmenkonzepte oder individuell entwickelte angemessene CMS-Grundsätze in Betracht. Bei der individuellen Entwicklung von CMS-Grundsätzen können die gesetzlichen Vertreter auch entscheiden, sich an verfügbaren Informationen über die Praxis anderer Unternehmen zu orientieren (vgl. Tz. A32). Sofern das angewandte Rahmenkonzept nicht alle CMS-Grundelemente (vgl. Tz. 27) 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.

A13 Allgemein anerkannte Rahmenkonzepte i.S. der Tz. 13f) werden – soweit nicht rechtlich vorgeschrieben – im Rahmen eines transparenten Verfahrens entwickelt, das die Veröffentlichung als Entwurf mit Möglichkeit der Kommentierung durch Fachkreise und die interessierte Öffentlichkeit beinhaltet. Die in der Anlage 1 nicht abschließend aufgeführten Rahmenkonzepte genügen diesen Anforderungen.

A14 Die CMS-Beschreibung (vgl. Tz. 13g)) stellt die Konzeption des CMS und die implementierten Regelungen des CMS in einer für die Nutzer verständlichen Art und Weise dar. Hierbei werden sowohl hinsichtlich des Umfangs als auch der Konkretisierung die Ziele des CMS sowie Art und Umfang der Geschäftstätigkeit des Unternehmens angemessen berücksichtigt. Regelmäßig wird die CMS-Beschreibung eine Zusammenfassung der relevanten internen Verfahrensbeschreibungen enthalten. Die CMS-Beschreibung wird im Allgemeinen aber nicht den Umfang einer umfassenden Prozessbeschreibung haben (vgl. Tz. 16). Sofern ausnahmsweise Verweise in der CMS-Beschreibung auf andere Dokumente erfolgen, ist die CMS-Beschreibung aus sich heraus verständlich und enthält alle wesentlichen Regelungen.

Die CMS-Beschreibung für einen zu prüfenden Teilbereich kann Teil einer übergeordneten Beschreibung des gesamten CMS des Unternehmens sein, sofern klar erkennbar ist, welche Darstellungen in der CMS-Beschreibung Gegenstand der Prüfung sind (vgl. Tz. A76 und Tz. A70).

A15 Eine falsche Darstellung in der CMS-Beschreibung (vgl. Tz. 13i)) kann z.B. vorliegen, wenn die CMS-Beschreibung

- nicht auf sämtliche Grundelemente eingeht,
- einen Mangel in dem in der CMS-Beschreibung dargestellten CMS nicht erkennen lässt oder
- unangemessene Verallgemeinerungen bzw. unausgewogene und verzerrende Darstellungen enthält.

A16 Unternehmen (vgl. Tz. 14) i.S. dieses *IDW Prüfungsstandards* können neben Unternehmen im rechtlichen Sinne auch Gesellschaften bürgerlichen Rechts, rechtsfähige bzw. nicht rechtsfähige Vereine, Stiftungen, Gebietskörperschaften, sonstige Körperschaften, Eigenbetriebe, Anstalten des öffentlichen Rechts, Gemeinschaften, natürliche Personen oder sonstige wirtschaftlich abgegrenzte Geschäftstätigkeiten (z.B. Standorte, selbstständige Teilbetriebe, Sparten) oder Gruppen dieser Einheiten sein.

Gegenstand, Ziel und Umfang der Prüfung [Tz. 15 ff.]

A17 Art und Umfang der gemäß Tz. 16 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 Wirksamkeit des CMS gegenüber Dritten).

A18 Bei der Beurteilung, ob ein angemessen dokumentiertes CMS vorliegt, ist zu berücksichtigen, dass eine fehlende oder unvollständige Dokumentation des CMS zu Zweifeln an der dauerhaften Funktionsfähigkeit der eingerichteten Regelungen führen kann. Zum Nachweis der jederzeitigen Angemessenheit des CMS im Zeitablauf und der kontinuierlichen Anwendung der Regelungen kann es sinnvoll sein, auch die laufenden Unterlagen über die Feststellung von Compliance-Risiken, deren Bewertung und Analyse sowie deren Kommunikation, die Einführung und Kommunikation des Compliance-Programms sowie die Regelungen zur Überwachung und Verbesserung des Systems unbeschadet anderer Aufbewahrungspflichten über einen ausreichend langen Zeitraum aufzubewahren.

A19 Eine „projektbegleitende“ Prüfung der Angemessenheit i.S. der Tz. 20 stellt keine Mitwirkung an der Entwicklung oder Einrichtung eines CMS dar, durch die der CMS-Prüfer aufgrund der Unabhängigkeitsvorschriften von einer späteren Prüfung der Wirksamkeit des CMS ausgeschlossen wäre. Werden bei der Prüfungsdurchführung wesentliche Mängel in dem in der CMS-Beschreibung dargestellten CMS erkannt, ist es mit der Stellung eines CMS-Prüfers vereinbar, Entscheidungsempfehlungen über notwendige Regelungen zur Ausgestaltung eines angemessenen CMS zu geben. Die Entscheidung über deren Annahme verbleibt beim Unternehmen. Entscheidungen über deren Umsetzung dürfen nicht vom CMS-Prüfer veranlasst werden.

A20 Hinreichende Sicherheit bedeutet nicht absolute Sicherheit: Auch ein wirksames 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 Zusammenwirken zweier oder mehrerer Personen oder dem Verzicht des Managements auf bestimmte Maßnahmen, weil die Kosten dafür höher eingeschätzt werden als der erwartete Nutzen.

A21 Der Kreis der „betroffenen Personen“ (vgl. Tz. 25) ist nicht notwendigerweise auf die vom Unternehmen beschäftigten Mitarbeiter begrenzt. Zum Beispiel kommen auch Mitarbeiter eines Zulieferers des Unternehmens als von den Grundsätzen und Maßnahmen Betroffene in Betracht, wenn dies mit dem Zulieferer vertraglich vereinbart wurde.

Grundelemente eines CMS [Tz. 27]

A22 Während die Grundelemente den Prozess für die Einrichtung eines CMS allgemein (als Referenzrahmen) beschreiben, werden durch die CMS-Grundsätze (vgl. Tz. 13e)) konkrete inhaltliche Anforderungen an das System definiert, die bei der Einrichtung zugrunde gelegt werden.

Compliance-Kultur

A23 Die Compliance-Kultur ist integrativer Bestandteil der Unternehmenskultur und enthält im Wesentlichen Merkmale, welche für die Einhaltung von Regeln im Unternehmen von besonderer Relevanz sind. Sie kann grundsätzlich nicht losgelöst betrachtet werden von anderen – die Kultur prägenden – Determinanten eines Unternehmens, vor allem solchen mit Einfluss auf das interne Risikomanagement- und Kontrollumfeld (Risikokultur, Kontrollkultur, Revisionskultur etc.). „Kulturprägende“ Determinanten können (neben den unten aufgeführten Merkmalen der Compliance-Kultur) u.a. sein:

- die Vermittlung und Akzeptanz von Vision, Leitbild und Wertesystem des Unternehmens
- die Art und Weise der Entscheidungsfindung im Unternehmen
- die glaubwürdige Übernahme unternehmerischer Sozialverantwortung (z.B. ESG-Grundsätze)
- die Bereitschaft zur Übernahme von Verantwortung auf Mitarbeiterebene – über den eigenen Bereich hinaus
- die Förderung einer konstruktiven Fehlerkultur
- die Art und Weise des Umgangs mit internen und externen Konflikten.

Die Angemessenheit und Wirksamkeit des CMS wird wesentlich durch die Compliance-Kultur im Unternehmen geprägt. Die Compliance-Kultur eines Unternehmens wird dabei im Wesentlichen bestimmt durch den gelebten Wertekanon des Unternehmens und seiner Mitarbeiter sowie den gesamtgesellschaftlichen Kontext, in dem es sich bewegt.

Eine authentische Compliance-Kultur lebt von einer regelmäßigen bewussten Reflektion der kulturellen Rahmenbedingungen der Organisation. Zu diesem Zweck kann es erforderlich sein, die Compliance-Kultur zu operationalisieren, bspw. durch:

- eine auf Leitungsebene angesiedelte organisatorische Verankerung, durch welche sie regelmäßig behandelt wird

- Entwicklung eines Zielbildes zur angestrebten Compliance-Kultur in Abstimmung mit anderen Governance-Funktionen und der Personalentwicklung (u.a. ableitbar aus Ursachenanalysen zu Fehlverhalten in der Vergangenheit)
- Entwicklung dokumentierter Grundlagen und Leitlinien zur angestrebten Compliance-Kultur unter Berücksichtigung bereichsspezifischer Risikostrukturen sowie der ggf. bereits existierenden Verlautbarungen in Kodizes und Leitbildern
- Etablierung von Kommunikationsmechanismen und Berichtswegen zur Umsetzung der Leitlinien und einer regelmäßigen Reflektion der gelebten Compliance-Kultur
- Regelmäßige kritische Hinterfragung der Ursachen von Fehlverhalten („Root Cause Analysis“) sowie Etablierung einer offenen und positiv geprägten Fehlerkultur („Lessons learned“ Prozess)

Die Compliance-Kultur wird z.B. durch folgende Merkmale beeinflusst:

- das die Compliance-relevanten Unternehmenswerte vermittelnde Verhalten der gesetzlichen Vertreter (Vorbildfunktion)
- die Aufstellung, Kommunikation und beispielhafte Vermittlung klarer und widerspruchsfreier Verhaltensgrundsätze, welche die angestrebte Umsetzung der proklamierten (Compliance-relevanten) Unternehmenswerte in der Praxis transparent machen
- das integre, verantwortungsvolle und werteorientierte Verhalten der Mitglieder des Managements auf allen Managementebenen im Einklang mit den zu beachtenden Regeln („Tone from the Top/Middle“)
- die Anreizsysteme, mit denen regelwidriges Verhalten verhindert und regelkonformes Verhalten gefördert wird, einschließlich der Berücksichtigung von Werteorientierung und Compliance im Einstellungsprozess, bei Personalbeurteilungen und Beförderungen
- der Führungsstil und die Personalpolitik des Unternehmens (z.B. Bedeutung der Kompetenz und Erfahrung der Mitarbeiter)
- die (Ermöglichung der) Bereitschaft der Mitarbeiter zur Ansprache von (Compliance-) Risiken und erkanntem Fehlverhalten unter Nutzung eines Hinweisgebersystems sowie
- die Stellung des und die Art der Aufgabenwahrnehmung durch das Aufsichtsorgan im Zusammenhang mit „Good Corporate Governance“ und Compliance.

In einer günstigen Compliance-Kultur, in der die Beachtung der relevanten Regeln eine hohe Bedeutung hat und aufgedeckte Regelverstöße ohne Ansehen der Person und von Hierarchien angemessene Sanktionen nach sich ziehen, werden die im CMS verankerten Regelungen von den Mitarbeitern eher beachtet.

Compliance-Ziele

A24 Die Festlegung der Compliance-Ziele, die mit dem CMS erreicht werden sollen, erfolgt in Übereinstimmung mit den allgemeinen Unternehmenszielen sowie mit der Unternehmensstrategie und umfasst insb. eine Analyse und Gewichtung der für das Unternehmen bedeutsamen Regeln.

Um für einzelne Regelungsbereiche Compliance-Ziele festzulegen, bietet es sich an, zunächst die jeweiligen Regelungsbereiche zu identifizieren und abzugrenzen. Zudem bietet es sich an, eine erste Risikoanalyse auf Gesamtunternehmensebene durchzuführen, um die Bereiche zu

identifizieren, für die aufgrund von Risikoabwägungen die Einrichtung besonderer Regelungen erforderlich erscheint. Faktoren, die bei der Festlegung der Compliance-Ziele eine Rolle spielen können, sind z.B., ob

- Erkenntnisse über Regelverstöße aus der Vergangenheit („Risiko-Historie“) vorliegen,
- ein Regelverstoß zu einer operativen Beeinträchtigung der Geschäftstätigkeit führen kann,
- ein Regelverstoß Gefahren für Leib und Leben von Mitarbeitern oder Dritten nach sich ziehen kann,
- ein Regelverstoß strafrechtliche Folgen für Mitarbeiter oder Dritte bedingen kann oder
- aus dem Regelverstoß ein materieller Reputationsschaden bzw. ein finanzieller Schaden für das Unternehmen erwachsen kann.

Darauf aufbauend können für die identifizierten Regelungsbereiche die jeweiligen Compliance-Ziele (ggf. für einzelne Organisationseinheiten) festgelegt werden (z.B. Einhaltung des Foreign Corrupt Practices Act – FCPA oder des UK-Bribery Act durch den Vertrieb). Gegenstand der Festlegung von Compliance-Zielen kann zudem auch sein, auf welche Weise sich abzeichnende Compliance-Risiken einer Risikosteuerung (Risikovermeidung, -reduktion, -teilung, -transfer oder -vorsorge) unterliegen sollen (z.B. Risikovermeidung durch den Verzicht einer Markterschließung in Ländern ab einem bestimmten CPI-Wert (Corruption Perceptions Index, CPI) oder Reduktion eines Geldwäscherisikos durch den Verzicht von Bargeldtransaktionen mit bestimmten risikobehafteten Kundengruppen). Bei der Festlegung der Compliance-Ziele sind ferner die folgenden Aspekte von Bedeutung:

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

Die für die abgegrenzten Regelungsbereiche festgelegten Compliance-Ziele sind die Grundlage für die weitergehende systematische Aufnahme und Beurteilung der Risiken für Regelverstöße (vgl. Tz. 27 (Compliance-Risiken)). Aus dieser regelmäßigen Befassung mit den Compliance-Risiken können sich im Zeitablauf auch Rückwirkungen auf die Festlegung der Compliance-Ziele für die jeweiligen Regelungsbereiche ergeben.

Compliance-Risiken

A25 Die Identifikation und Beurteilung von Compliance-Risiken sind der Ausgangspunkt für die Entwicklung eines angemessenen Compliance-Programms.

Das Unternehmen führt zu diesem Zweck für die abgegrenzten relevanten Regelungsbereiche des CMS (vgl. Tz. 27 (Compliance-Ziele)) eine systematische Aufnahme bzw. Identifikation der Risiken für Regelverstöße durch, z.B. in Form von Interviews, Workshops oder der Auswertung von verfügbaren Informationen anderer Unternehmen.

Die Risikobeurteilung kann auf Basis eines systematischen Verfahrens erfolgen, bei dem z.B. auf qualitative Kriterien (z.B. Expertenschätzung), quantitative Kriterien (z.B. Anzahl der

Geldwäscheverdachtsmeldungen) oder semi-quantitative Kriterien (z.B. Anwendung von Scoring Modellen) zurückgegriffen werden kann. Bei der Risikobeurteilung werden die grundsätzlichen Entscheidungen der gesetzlichen Vertreter zur Risikosteuerung (Risikovermeidung, -reduktion -teilung, -transfer oder -vorsorge) berücksichtigt. Bei einer Akzeptanz von Compliance-Risiken berücksichtigt das Unternehmen insb., ob dies mit dem bestehenden Ermessensspielraum bei den Sorgfalts- und Organisationspflichten vereinbar ist bzw. ein Compliance-Risiko durch entsprechende Steuerungsmaßnahmen auf ein vertretbares Maß reduziert wurde.

Mögliche Risikointerdependenzen (Risiken, die in Abhängigkeit zueinander stehen oder sich gegenseitig beeinflussen) und damit einhergehende Änderungen der Risiko-Expositionen sind ebenfalls bei der Beurteilung zu berücksichtigen.

Die Beurteilung kann z.B. in einem zweistufigen Verfahren erfolgen, indem zunächst eine Beurteilung der Risiko-Eintrittswahrscheinlichkeit und des potenziellen Schadensausmaßes (insb. mit Blick auf einen möglichen wirtschaftlichen, reputativen oder regulatorischen Schaden) vor möglichen Maßnahmen zur Risikosteuerung (sog. Brutto-Risiko) erfolgt. In einem zweiten Schritt kann dann eine erneute Beurteilung unter Berücksichtigung von Maßnahmen zur Risikosteuerung (Netto-Risiko) erfolgen.

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

- Größe, Komplexität und Struktur des Unternehmens,
- Grad der Delegation von Aufgaben,
- Branche und Betätigungsfelder des Unternehmens,
- Art und Umfang der Geschäftstätigkeit (insb. Produkte, Dienstleistungen, Transaktionen und Vertriebskanäle) des Unternehmens,
- Geschäftspartner (Kunden, Lieferanten, Dienstleister)
- Geographische Ausrichtung der Geschäftstätigkeit,
- Änderungen im wirtschaftlichen und rechtlichen Umfeld,
- Personalveränderungen,
- überdurchschnittliches Unternehmenswachstum,
- neue Technologien,
- Akquisitionen und Umstrukturierungen,
- Kenntnisse der Mitarbeiter über die zu beachtenden Regelungen,
- Führungsstil 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.

Es bietet sich an, eine „Risiko-Kontroll-Matrix“ zu erstellen, mittels derer den Risiken entsprechende Maßnahmen des Compliance-Programms gegenübergestellt werden (vgl. Tz. A26).

Compliance-Programm

A26 Ein Compliance-Programm setzt sich aus den Regelungen zusammen, die von dem Unternehmen zur Verhinderung oder Begrenzung der Compliance-Risiken eingerichtet werden und auf ein regelkonformes Verhalten abzielen.

Diese Regelungen umfassen z.B. Richtlinien, Arbeitsanweisungen, Handbücher oder Kontrollbeschreibungen, die den Mitarbeitern klare Vorgaben zu den einzuhaltenden Prozessen, durchzuführenden Kontrollen sowie zur Zulässigkeit bzw. Unzulässigkeit bestimmter Aktivitäten machen.

Das Compliance-Programm beinhaltet klare Vorgaben zur Verhinderung spezifischer Compliance-Verstöße, z.B. durch Freigaberegelungen bzw. durch die Kenntnis der Mitarbeiter, dass nachgelagerte Kontrollen existieren. Des Weiteren kann die Einbindung der Compliance-Funktion (z.B. eines Compliance-Beauftragten bzw. einer Compliance-Abteilung oder eines Compliance-Gremiums) in relevante Vorgänge eine mögliche vorbeugende Maßnahme darstellen. Zum Compliance-Programm gehört regelmäßig auch die Festlegung eines Schulungskonzepts.

Das Compliance-Programm umfasst auch Maßnahmen, die darauf ausgerichtet sind, mögliche Compliance-Verstöße rechtzeitig zu erkennen und zu melden (z.B. die Einrichtung eines Hinweisgeberverfahrens) und Reaktionen auf die möglichen Compliance-Verstöße. Ein Hinweisgeberverfahren[20] wird klar an die Mitarbeiter kommuniziert und macht deutlich, dass keine negativen Konsequenzen für den meldenden Mitarbeiter bei einer begründeten Meldung erfolgen. Es zeichnet sich dadurch aus, dass die Vertraulichkeit der Identität des Hinweisgebers und Dritter, die in der Meldung erwähnt werden, gewahrt bleibt und nicht befugten Mitarbeitern der Zugriff darauf verwehrt wird. Für den Fall der Aufdeckung von Regelverstößen ist eine zeitnahe Kommunikation an die zuständigen Stellen im Unternehmen und erforderlichenfalls an externe Stellen (z.B. bei Verdacht auf Verstöße gegen das Geldwäschegesetz) vorgesehen.

Bei erwiesenen Verstößen erfolgt eine detaillierte Analyse der Ursachen für die Regelverstöße. Ursachen können hierbei z.B. neben prozessualen Schwächen auch Kontrollversagen oder individuelles Fehlverhalten sein. Nach Abschluss der Ursachenanalyse wird darauf hinzuwirken sein, dass der Verstoß nicht erneut im Unternehmen auftreten kann. Die Ursachenanalyse stellt eine wesentliche Grundlage für die kontinuierliche Verbesserung des CMS dar.

Zum Compliance-Programm zählen auch die integrierten Kontrollen, mit denen die Einhaltung der Regelungen und die Durchführung der Maßnahmen sichergestellt werden. Hierbei handelt es sich z.B. um

- Funktionstrennungen,

[20] Der Referentenentwurf eines Hinweisgeberschutzgesetzes, mit dem insb. die EU-Whistleblower-Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden („EU-Whistleblower Richtlinie 2019/1937"), umgesetzt werden soll, sieht vor, dass insb. alle Unternehmen aus dem Bereich der Finanzdienstleistungen ein internes bzw. externes Hinweisgebersystem einrichten müssen, mit dem Verstöße gegen nationales oder EU-Recht des Unternehmens gemeldet werden können. Dies gilt insoweit unabhängig von der Anzahl der beschäftigten Mitarbeiter. Alle weiteren Unternehmen mit mindestens 50 Mitarbeitern müssen ebenfalls ein internes bzw. externes Hinweisgebersystem einrichten.

- Berechtigungskonzepte,
- Genehmigungsverfahren und Unterschriftsregelungen,
- Vorkehrungen zum Vermögensschutz und andere Sicherheitskontrollen,
- unabhängige Gegenkontrollen (Vier-Augen-Prinzip) und
- Job-Rotationen.

Im Folgenden sind als „Risiko-Kontroll-Matrix“ beispielhaft und vereinfacht (z.B. ohne Berücksichtigung der Ergebnisse der Risikobeurteilung oder einer Zuordnung von Verantwortlichkeiten) für verschiedene Rechtsgebiete und im Unternehmen auftretende Risiken entsprechende Regelungen eines Compliance-Programms gegenübergestellt:

Rechtsgebiet	**Risiko**	**Programm**
Antikorruption	● Unangemessene Einladungen/Essenseinladungen oder sonstige Zuwendungen werden dazu genutzt, Geschäftspartner zu bestechen	● Zuwendungsrichtlinie inkl. Wertgrenzen und Freigabeprozesse (Freigabe durch Vorgesetzten oder Compliance Officer je nach Schwellenwert) ● Detektivisch: stichprobenartige Auswertung der Bewirtungsaufwendungen auf Einhaltung der Richtlinienvorgaben ● Sensibilisierungsmaßnahmen ● Implementierung eines Hinweisgeberverfahrens zur Meldung von Verdachtsfällen/Verstößen
Antikorruption	● Existenz bzw. Eingehen von Scheinberaterverträgen	● Business Partner Due Diligence ● Mehr-Augenprinzip bei Auftragsvergabe ● Überprüfung der Leistungserbringung vor Zahlung ● Sensibilisierungsmaßnahmen ● Implementierung eines Hinweisgeberverfahrens zur Meldung von Verdachtsfällen/Verstößen
Antikorruption	● Missbrauch von Spenden- oder Sponsoringzahlungen	● Spenden- und Sponsoringrichtlinie und Freigabeprozesse ● Compliance-Prüfung des Empfängers ● Sensibilisierungsmaßnahmen ● Implementierung eines Hinweisgeberverfahrens zur Meldung von Verdachtsfällen/Verstößen

Rechtsgebiet	Risiko	Programm
Kartellrecht	● Unangemessene Absprachen (Preis, Technik) (z.B. durch Fehlverhalten auf Verbandstreffen)	● Richtlinie ● Übersicht der Verbände (Prüfung der Agenda und Protokolle, Freigabe der Teilnahme) ● Sensibilisierungsmaßnahmen (z.B. Schulungen) insb. von Mitarbeitern, die in stärkerer Weise kartellrechtlichen Risiken ausgesetzt sind (z.B. im Vertrieb oder Teilnehmer von Verbandstreffen bzw. Branchentagungen) ● Implementierung eines Hinweisgeberverfahrens zur Meldung von Verdachtsfällen/Verstößen
Exportkontrolle	● Warenlieferung/Dienstleistungen an Embargoländer oder sanktionierte Personen	● IT-gestütztes Sanktionslistenscreening (Datenbanken) ● Sensibilisierungsmaßnahmen ● Implementierung eines Hinweisgeberverfahrens zur Meldung von Verdachtsfällen/Verstößen
Exportkontrolle	● Verstoß gegen dual-use Verordnung	● Systematischer Prozess zur Identifikation von dual-use Gütern ● Sensibilisierungsmaßnahmen ● Implementierung eines Hinweisgeberverfahrens zur Meldung von Verdachtsfällen/Verstößen
Geldwäsche	● Annahme von Bargeldgeschäften über 10.000 € ohne angemessene Geschäftspartnerprüfung	● Richtlinie zur Geldwäsche ● Keine Möglichkeit, Bargeld einzuzahlen ● Business Partner Due Diligence (IT-gestützt) ● Implementierung eines Hinweisgeberverfahrens zur Meldung von Verdachtsfällen/Verstößen
Product Compliance	● Gesetzliche Anforderungen an die Beschaffenheit eines Produktes werden nicht erfüllt	● Systematisches und kontinuierliches Monitoring der gesetzlichen Anforderungen ● Prüfung von Produktänderungen und entsprechende Freigabe ● Prozess zur Interpretation von Gesetzesauslegungen ● Implementierung eines Hinweisgeberverfahrens zur Meldung von Verdachtsfällen/Verstößen

Weitere konkrete Beispiele für die Bestandteile von Compliance-Programmen sind in den in der Anlage 1 aufgeführten CMS-Rahmenkonzepten sowie in den in der Anlage 2 aufgeführten Hinweisen und Hilfestellungen zur Ausgestaltung von CMS enthalten.

Compliance-Organisation

A27 Merkmale einer Compliance-Organisation sind u.a.

- die klare Festlegung von Rollen und Verantwortlichkeiten im CMS, z.B. die Bestimmung eines Compliance-Beauftragten bzw. eines Compliance-Gremiums einschließlich der Festlegung der Aufgaben und der hierarchischen Stellung bzw. der organisatorischen Einordnung sowie der Berichtslinien. Die Festlegung der Rollen und Verantwortlichkeiten wird in der Praxis zum Teil anhand des „Three-lines-Modells" vorgenommen. In kleineren Unternehmen werden Aufgaben des Compliance-Managements zum Teil zentral von der Geschäftsführung selbst wahrgenommen.
- der Compliance-Funktion (vgl. Tz. A26) zugeordnete Mitarbeiter haben die notwendige Unabhängigkeit, Kompetenz und organisatorische Stellung, um ihre Rollen und Verantwortlichkeiten wirksam wahrzunehmen. Dazu gehört auch die Möglichkeit zur unmittelbaren Kommunikation mit den gesetzlichen Vertretern bzw. den für die Überwachung Zuständigen sowie die rechtzeitige Einbindung in langfristige Entscheidungsprozesse.
- die Bereitstellung von im Hinblick auf die Compliance-Ziele und Compliance-Risiken ausreichenden personellen und ggf. technischen Ressourcen zur Konzeption, Einführung, Durchsetzung und Überwachung sowie kontinuierlichen Verbesserung des CMS,
- die Integration des CMS in die Geschäftsprozesse des Unternehmens und in andere bestehende Systeme der Unternehmensüberwachung, wie z.B. das Risikomanagementsystem, und
- die Entwicklung und Einsatz 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 (z.B. web-basierte Abfragesysteme und Controllingsysteme) handeln.

Compliance-Kommunikation

A28 Die Compliance-Kommunikation kann u.a. die folgenden Elemente umfassen:

- Kommunikation der Unternehmenswerte, der Compliance-Kultur und erwarteter Verhaltensweisen an die Mitarbeiter und ggf. Dritte durch das Management
- Kommunikation der in den Teilbereichen zu beachtenden Regeln sowie des Compliance-Programms an die betroffenen Personen (speziell auch für neue Mitarbeiter oder ggf. Dritte) sowie der Beratungsfunktion von Compliance
- Aus- und Weiterbildung der Mitarbeiter und ggf. Dritter zur Erkennung von Compliance-Risiken und dem Umgang mit solchen auf Basis der Compliance-Kultur sowie des Compliance-Programms

- Festlegung der Berichtspflichten (Anlässe) und der Berichtswege für die Information und 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 sowohl an das Management als auch in geeigneter, ggf. abweichender Form an Mitarbeiter.

Die Compliance-Kommunikation erfolgt regelmäßig und strukturiert und kann z.B. in Form von Mitarbeiterbriefen, Compliance-Handbüchern oder im Rahmen von Schulungsveranstaltungen erfolgen. Sofern möglich, wird regelkonformes Verhalten durch das Management sowie das Aufsichtsorgan regelmäßig auch unmittelbar gegenüber den Mitarbeitern kommuniziert und betont.

Die Frequenz der Kommunikation sowie der Detailgrad richtet sich nach Art und Umfang der Compliance-Risiken und ist den speziellen Risiken der Empfänger(-gruppen) angepasst. Bei besonders exponierten Personen kann sich eine individuell zugeschnittene und ggf. ereignisorientierte Kommunikation anbieten.

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. Dies kann durch geeignete Maßnahmen unterstützt werden.

Sofern praktikabel, bestätigen die Mitarbeiter und ggf. Dritte die Kenntnisnahme der Kommunikation (z.B. durch Teilnahmelisten bei Schulungsveranstaltungen oder Unterzeichnung eines Formulars zur Einhaltung relevanter Grundsätze). Eine wirksame Compliance-Kommunikation ist auch dadurch gekennzeichnet, dass über die bloße Kenntnisnahme hinaus das inhaltliche Verständnis nachgewiesen wird (z.B. durch Mitarbeiterbefragungen oder Onlinetests).

Compliance-Überwachung und Verbesserung

A29 Die Compliance-Überwachung zielt darauf ab festzustellen, ob das CMS unter Beachtung der angewandten CMS-Grundsätze angemessen ausgestaltet und wirksam ist. Bei der Compliance-Überwachung handelt es sich zum einen um Überwachungsmaßnahmen durch prozessunabhängige Stellen, z.B. die Interne Revision. Zudem beinhaltet die Überwachung auch, ob die prozessintegrierten Kontrollen (vgl. Tz. A26) 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 (Ursachenanalyse). 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, werden als Bestandteil der Durchsetzung des CMS erkennbare Maßnahmen getroffen, 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 Regelverstößen bzw. bei Missachtung wesentlicher Regelungen des CMS kann auch die Kündigung des Arbeitsvertrags oder die Kündigung von Verträgen mit Dritten in Betracht kommen.

Das Aufsichtsorgan wird über die Maßnahmen zur Überwachung und Verbesserung des CMS informiert, soweit es der Erfüllung der eigenen Überwachungsfunktion des Aufsichtsorgans dient (z.B. § 107 Abs. 3 AktG). Entsprechend kann das Aufsichtsorgan von seinem unmittelbaren Auskunftsrecht nach § 107 Abs. 4 Satz 4 AktG, z.B. gegenüber dem CMS-Verantwortlichen oder dem Leiter der Internen Revision Gebrauch machen.

Auftragsannahme [Tz. 29 ff.]

A30 Folgende Aspekte haben bei der Beurteilung der Eignung des in der CMS-Beschreibung dargestellten Systems als Prüfungsgegenstand eine besondere Bedeutung (vgl. Tz. 32):

- Übernehmen die gesetzlichen Vertreter Verantwortung für Einrichtung, Aufrechterhaltung, Überwachung und Durchsetzung des CMS?
- Ist das CMS in einer Weise dokumentiert, dass ein sachverständiger Dritter in angemessener Zeit einen Überblick über das 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 werden geeignete CMS-Grundsätze verwendet (vgl. Tz. 13e) und Anlage 1)?
- Sind die zur Anwendung kommenden CMS-Grundsätze den beabsichtigten Berichtsadressaten zugänglich?

A31 Die grundsätzliche Eignung des in der CMS-Beschreibung dargestellten Systems als Prüfungsgegenstand kann dadurch beeinträchtigt werden, dass eine von den gesetzlichen Vertretern festgelegte Abgrenzung der zu prüfenden Teilbereiche nicht hinreichend klar bzw. irreführend ist.

A32 Im Rahmen der Prüfung der Eignung der zugrunde gelegten CMS-Grundsätze ist von Bedeutung, ob die in der CMS-Beschreibung dargestellten CMS-Grundsätze gesetzlich vorgeschrieben sind oder ob sie auf einschlägigen, allgemein anerkannten Rahmenkonzepten oder auf anderen themen-, branchen- oder industriespezifischen Rahmenkonzepten beruhen (vgl. Anlage 1). Sofern solche Rahmenkonzepte nicht existieren oder nicht ausreichend konkret sind, können auch entsprechende Grundsätze durch das Unternehmen selbst entwickelt oder ergänzt werden. Sofern keine gegenteiligen Anhaltspunkte vorliegen, ist davon auszugehen,

dass durch Gesetz oder andere Rechtsvorschriften vorgeschriebene CMS-Grundsätze geeignet sind. Solche CMS-Grundsätze werden als anerkannte CMS-Grundsätze angesehen.

Bei der Entwicklung von individuellen CMS-Grundsätzen kann sich das Unternehmen an den CMS-Grundelementen (vgl. Tz. 27) orientieren.

A33 Geeignete CMS-Grundsätze i.S. dieses *IDW Prüfungsstandards* erfüllen die folgenden Merkmale:

- *Relevanz:* Relevante CMS-Grundsätze führen zu Informationen über das CMS, die die Entscheidungsfindung der Nutzer der CMS-Beschreibung unterstützen.
- *Vollständigkeit:* CMS-Grundsätze sind vollständig, wenn die nach diesen Grundsätzen erstellten Informationen keine relevanten Gesichtspunkte ausklammern, von denen angenommen werden kann, dass sie die Entscheidungsfindung der Nutzer beeinflussen würden.
- *Verlässlichkeit:* CMS-Grundsätze führen bei der Anwendung in vergleichbaren Fällen zu einer hinreichend konsistenten Beurteilung des CMS.
- *Neutralität:* CMS-Grundsätze führen zu Informationen, die frei von einseitigen Darstellungen sind.
- *Verständlichkeit:* CMS-Grundsätze führen zu nachvollziehbaren und verständlichen Informationen für die Nutzer der CMS-Beschreibung.

A34 Folgende Aspekte werden im Allgemeinen mit dem Auftraggeber schriftlich vereinbart:

- Ziel und Gegenstand der CMS-Prüfung (vgl. Tz. 15 ff.)
- die Verantwortung der gesetzlichen Vertreter für das CMS einschließlich der Abgrenzung der Teilbereiche und der Dokumentation des CMS sowie für die Inhalte der CMS-Beschreibung (vgl. Tz. 16)
- die vom Unternehmen angewandten CMS-Grundsätze
- Art und Umfang der Prüfung des CMS und der Berichterstattung einschließlich einer Bezugnahme auf diesen *IDW Prüfungsstandard*; dies bezieht sich auch auf die Berichterstattung über festgestellte Regelverstöße (vgl. Tz. 63, Tz. 110)
- die Tatsache, dass die Prüfung der Darstellungen in der CMS-Beschreibung risikoorientiert erfolgt und keine Vollprüfung, sondern eine Prüfung in einer Auswahl vorgenommen wird und deshalb ein unvermeidbares Risiko besteht, dass selbst wesentliche falsche Darstellungen in der CMS-Beschreibung bzw. wesentliche Mängel im CMS unentdeckt bleiben können
- ein Hinweis auf die systemimmanenten Grenzen eines CMS (vgl. Tz. A20) und dass die Prüfung nicht darauf ausgerichtet ist, einzelne Regelverstöße aufzudecken
- bei einer Angemessenheitsprüfung: Zeitpunkt, auf den sich die Prüfung der Angemessenheit beziehen soll
- bei einer Wirksamkeitsprüfung: Zeitraum, auf den sich die Prüfung der Wirksamkeit des CMS beziehen soll
- Hinweise auf die Nutzung von Arbeiten der Internen Revision, anderer Wirtschaftsprüfer sowie von Sachverständigen

- 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 für den Auslagenersatz
- Haftungsbeschränkungen
- die Verpflichtung der gesetzlichen Vertreter, eine Vollständigkeitserklärung abzugeben
- ggf. Verwendungsvorbehalt des CMS-Prüfungsberichts sowie
- ggf. Hinweis auf Berichtspflichten gegenüber dem Aufsichtsorgan.

A35 Wenn der CMS-Prüfer auch mit anderen Dienstleistungen (z.B. der Abschlussprüfung) beauftragt war und er in deren Rahmen für die Beurteilung der Darstellungen in der CMS-Beschreibung evtl. relevante Informationen erlangt hat, kann es sinnvoll sein, zu vereinbaren, dass er das Ergebnis dieser Tätigkeiten bei der Prüfung des CMS berücksichtigt.

A36 Es kann sinnvoll sein, im Rahmen der Auftragsannahme eine Vereinbarung mit dem Unternehmen über die Einbeziehung von sonstigen Informationen (vgl. Tz. 76) in die CMS-Prüfung zu schließen.

A37 Beispiele für Änderungen der Bedingungen des Prüfungsauftrags (vgl. Tz. 38) sind:

- Änderungen des in der CMS-Beschreibung dargestellten Umfangs des CMS (z.B. durch Ausklammerung bestimmter Regionen oder Länder).
- Anstelle einer Wirksamkeitsprüfung soll nur die Angemessenheit des CMS geprüft werden.

Prüfungsplanung [Tz. 39 ff.]

A38 Sachverständige (z.B. Rechtsexperten, Forensiker oder Datenanalyseexperten) können z.B. einbezogen werden, wenn Darstellungen zur Angemessenheit des CMS zur Verhinderung wirtschaftskrimineller Handlungen oder zur Einhaltung komplexer regulatorischer Anforderungen zu beurteilen sind.

A39 Die Verlässlichkeit der Informationen (vgl. Tz. 46), die als Prüfungsnachweise genutzt werden sollen, wird durch die Quelle und Art der Informationen sowie durch die Umstände beeinflusst, unter denen sie erlangt werden. Folgende allgemeine Aussagen hinsichtlich der Verlässlichkeit von Prüfungsnachweisen können nützlich sein:

- Die Verlässlichkeit von Prüfungsnachweisen nimmt zu, wenn diese aus unabhängigen Quellen außerhalb des Unternehmens stammen.
- Unmittelbar vom CMS-Prüfer erlangte Prüfungsnachweise (z.B. durch Beobachtung der Durchführung einer Kontrolle) sind verlässlicher als Prüfungsnachweise, die mittelbar oder durch Rückschluss (z.B. Befragungen über die Durchführung einer Kontrolle) erlangt werden.
- Prüfungsnachweise in dokumentierter Form, ob auf Papier, einem elektronischen oder anderen Medium, sind verlässlicher als mündlich erlangte Nachweise.
- Als Originaldokumente vorgelegte Prüfungsnachweise sind verlässlicher als Prüfungsnachweise, die als Fotokopien, digitalisierte oder anderweitig in eine elektronische Form

umgewandelte Dokumente vorgelegt werden, deren Verlässlichkeit von den Kontrollen über ihre Erstellung und Aufrechterhaltung abhängen kann.

Wesentlichkeit [Tz. 47]

A40 Der CMS-Prüfer berücksichtigt seine Überlegungen zur Wesentlichkeit

- bei der Planung und Durchführung der Prüfung, einschließlich der Bestimmung von Art, Umfang und zeitlicher Einteilung der Prüfungshandlungen, und
- bei der Auswertung von Prüfungsfeststellungen, d.h. bei der Beurteilung, ob die CMS-Beschreibung wesentliche falsche Darstellungen (vgl. Tz. 13i)) enthält bzw. ein festgestellter Mangel des CMS wesentlich ist, und
- bei der Würdigung von anlässlich der CMS-Prüfung festgestellten Regelverstößen.

A41 Eine wesentliche falsche Darstellung in der CMS-Beschreibung liegt z.B. dann vor, wenn

- sie einen vorhandenen wesentlichen Mangel des CMS nicht erkennen lassen,
- sie falsche Angaben enthalten oder Angaben fehlen, die – einzeln oder in der Summe – für die Adressaten der CMS-Beschreibung entscheidungsrelevant sein können, oder
- sie unangemessene Verallgemeinerungen oder unausgewogene und verzerrende Darstellungen enthalten, die eine Irreführung der Adressaten der CMS-Beschreibung zur Folge haben können.

A42 Ein wesentlicher Mangel des CMS liegt dann vor, wenn das in der CMS-Beschreibung dargestellte CMS nicht mit hinreichender Sicherheit sowohl Risiken für wesentliche Verstöße gegen die Regeln, auf deren Einhaltung das CMS in den vom Unternehmen abgegrenzten Teilbereichen ausgerichtet ist, rechtzeitig erkennt als auch solche Regelverstöße verhindert. Ein wesentlicher Mangel des CMS kann auch bei einer Kumulation von nicht rechtzeitig erkannten Risiken und nicht vom System verhinderten Regelverstößen vorliegen, die einzeln betrachtet nicht wesentlich sind.

A43 Bei der Bestimmung der Wesentlichkeit von (möglichen) Regelverstößen sind insb. folgende Fragestellungen von Bedeutung:

- *Bedeutung der verletzten Regel:* Handelt es sich um einen Verstoß gegen Rechtsvorschriften oder gegen interne Richtlinien?
- *Folgen des Regelverstoßes:* Ist mit dem Regelverstoß ein hoher finanzieller oder sonstiger Schaden für das Unternehmen oder ggf. Dritte verbunden?
- *Motivation für den Regelverstoß:* Handelt es sich um einen beabsichtigten Regelverstoß? Ist mit dem Regelverstoß eine persönliche Bereicherung oder ein sonstiger Vorteil verbunden?
- *Tragweite des Regelverstoßes:* Ist der Regelverstoß 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?

A44 Anhaltspunkte für wesentliche Mängel des in der CMS-Beschreibung dargestellten CMS können sich u.a. aus den folgenden Umständen ergeben:

- Es werden keine geeigneten CMS-Grundsätze verwendet (vgl. Tz. A32 f.).

- Die Konzeption des CMS weist Lücken auf, die dazu führen können, dass nicht alle Risiken für wesentliche Regelverstöße, die eine mehr als vertretbar niedrige Eintrittswahrscheinlichkeit haben, identifiziert werden, z.B. gibt es kein angemessenes Verfahren zur Meldung von Verdachtsfällen durch Mitarbeiter.
- Der Prozess zur systematischen Erfassung und Analyse von wesentlichen Compliance-Risiken weist Schwachstellen auf, z.B. werden im Rahmen der Prüfung wesentliche Compliance-Risiken erkannt, die vom CMS zuvor nicht erfasst und analysiert worden sind.
- Die Regelungen des CMS werden nicht regelmäßig auf Anpassungsbedarf wegen geänderter Rahmenbedingungen überprüft und ggf. geändert.
- Im CMS werden keine ausreichenden Ressourcen eingesetzt.
- Das CMS wird im Unternehmen nicht ausreichend kommuniziert und überwacht.
- Das CMS wird nicht konsequent durchgesetzt, z.B. wenn bei aufgedeckten Regelverstößen die Nichtbeachtung des CMS durch die Mitarbeiter keine wirksamen Konsequenzen hat.

Gewinnung eines Verständnisses von dem Unternehmen sowie von dessen rechtlichem und wirtschaftlichem Umfeld [Tz. 48 f.]

A45 Sofern es sich bei dem CMS-Prüfer um den Abschlussprüfer des Unternehmens handelt, wird das erforderliche Verständnis von dem rechtlichen und wirtschaftlichen Umfeld des Unternehmens und dem CMS teilweise bereits vorhanden sein.[21] Die Abschlussprüfung hat im Unterschied zur CMS-Prüfung allerdings das Ziel, die Ordnungsmäßigkeit der Rechnungslegung zu beurteilen. Der Abschlussprüfer richtet seine Risikobeurteilungen daher auf die Feststellung wesentlicher falscher Darstellungen in der Rechnungslegung aus. Das in diesem Zusammenhang erworbene Verständnis von dem Unternehmen, seines rechtlichen und wirtschaftlichen Umfelds und des rechnungslegungsbezogenen internen Kontrollsystems des Unternehmens wird für Zwecke der CMS-Prüfung im Allgemeinen nicht ausreichend sein.

A46 Das vom CMS-Prüfer zu erlangende Verständnis von dem Unternehmen sowie von dessen rechtlichem und wirtschaftlichem Umfeld ist abhängig von dem jeweiligen zu prüfenden Teilbereich und kann z.B. Aspekte wie das Unternehmensumfeld, wichtige Merkmale des Unternehmens, wie Rechtsform, Branche, Geschäftstätigkeit und -entwicklung, Eigentümerstruktur, Überwachungsstruktur, Finanzierung, Ziele und Strategien sowie Geschäftsrisiken umfassen.

A47 Besprechungen zwischen dem auftragsverantwortlichen Wirtschaftsprüfer und anderen Mitgliedern des Prüfungsteams sowie ggf. mit Sachverständigen des CMS-Prüfers verfolgen das Ziel, die Mitglieder für das mögliche Vorhandensein wesentlicher falscher Darstellungen in der CMS-Beschreibung bzw. wesentliche Mängel im CMS zu sensibilisieren und ihr Verständnis für die Auswirkungen der Ergebnisse ihrer Prüfungshandlungen auf andere Aspekte der CMS-Prüfung zu fördern.

[21] Vgl. ISA [DE] 315 (Revised) „Identifizierung und Beurteilung der Risiken wesentlicher falscher Darstellungen aus dem Verständnis von der Einheit und ihrem Umfeld.

Gewinnung eines Verständnisses von dem in der CMS-Beschreibung dargestellten CMS [Tz. 50 f.]

A48 Das vom CMS-Prüfer zu erlangende Detailverständnis von dem CMS umfasst z.B. folgende Aspekte:

- Die auf der Grundlage der allgemeinen Unternehmensziele sowie der Unternehmensstrategie und einer Analyse und Gewichtung der für das Unternehmen bedeutsamen Regeln festgelegten Compliance-Ziele,
- die Ausprägung des Risikobewusstseins der Mitarbeiter,
- die Aufbau- und Ablauforganisation des CMS,
- die Regelungen zur Erkennung und Verhinderung von Regelverstößen und
- die Regelungen zur Überwachung und Verbesserung des CMS.

Prüfungsdurchführung [Tz. 54 ff.]

Prüfung der in der CMS-Beschreibung enthaltenen Darstellungen zur Angemessenheit und Wirksamkeit des CMS [Tz. 57 ff.]

A49 Bei der Festlegung der Prüfungshandlungen kann der CMS-Prüfer bei wiederkehrenden Aufträgen Ergebnisse früherer CMS-Prüfungen nutzen, soweit die Ergebnisse aufgrund unveränderter Verhältnisse noch relevant sind. Dies gilt vor allem für die Beurteilung der Angemessenheit des CMS, die sich bei Folgeprüfungen vor allem auf Veränderungen des CMS erstrecken wird. In Bezug auf die Beurteilung der Wirksamkeit des CMS im Prüfungszeitraum können sich die Erkenntnisse aus früheren Prüfungen hauptsächlich auf die Risikobeurteilung des CMS-Prüfers und den Umfang der Prüfungen der Wirksamkeit auswirken. Prüfungsnachweise aus früheren Prüfungen stellen aber für sich genommen keinen Nachweis über die Wirksamkeit des CMS im zu prüfenden Zeitraum dar.

A50 Im Rahmen der Prüfung der Angemessenheit des CMS (vgl. Tz. 58) kommen insb. die folgenden Prüfungshandlungen in Betracht:

- Befragungen der gesetzlichen Vertreter, anderer Mitglieder des Managements und von Mitgliedern des Aufsichtsorgans (z.B. zur Konzeption des CMS, zur Durchsetzung des CMS, zu bekannten Schwachstellen im CMS),
- Befragungen von Personen, die für die Konzeption oder Weiterentwicklung, 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 im Compliance-Programm verankerte Regelungen sowie die Reaktionen des Unternehmens auf solche Feststellungen in Erfahrung zu bringen (z.B. Compliance-Beauftragter oder Interne Revision),
- Durchsicht von Dokumentationen des CMS (z.B. Organisationshandbücher, in denen Verantwortlichkeiten und Maßnahmen geregelt sind, sowie entsprechende Anweisungen an die Mitarbeiter),
- Durchsicht von Unterlagen, die durch das CMS generiert werden (z.B. Dokumentation zu festgestellten Regelverstößen und Sanktionen bei festgestellten Regelverstößen) und

- Beobachtung von Aktivitäten und Arbeitsabläufen im Unternehmen, die mit dem CMS in Verbindung stehen.

A51 Die Prüfung der Wirksamkeit (vgl. Tz. 60) umfasst die kontinuierliche Anwendung der im CMS verankerten Regelungen in dem von der Prüfung abgedeckten Zeitraum. Es wird geprüft, ob das Compliance-Programm wie vorgesehen von den dafür bestimmten Personen beachtet bzw. durchgeführt wurde und diesen die für die Wahrnehmung der Aufgaben erforderlichen Hilfsmittel und Informationen zur Verfügung standen.

A52 Folgende Prüfungshandlungen kommen im Rahmen der Prüfung der Wirksamkeit des CMS in Betracht:

- Befragung der von den Regelungen betroffenen Personen (gesetzliche Vertreter, Mitarbeiter im CMS, Mitarbeiter der Internen Revision und andere relevante Mitarbeiter)
- Durchsicht und Auswertung der CMS-Dokumentation hinsichtlich der kontinuierlichen Anwendung der Regelungen, z.B. Protokolle von Aufsichtsratssitzungen, Risikoinventaren, Checklisten, Fragebögen, Kontrollbeschreibungen, Berichte der Internen Revision
- Beobachtung der Einhaltung von Grundsätzen bzw. der Durchführung von Verfahren und Maßnahmen im CMS (z.B. Risk Assessment Diskussionen, Überwachungsmaßnahmen der Internen Revision)
- Nachvollziehen[22] („unabhängige Durchführung“) von für das CMS relevanten Verfahren und Kontrollen
- IT-gestützte Prüfungshandlungen (z.B. Datenanalysen im Zusammenhang mit systemtechnisch abgebildeten Berechtigungs- und Freigabekonzepten).

A53 Befragungen allein reichen für die Erzielung der erforderlichen Urteilssicherheit über die Wirksamkeit des CMS nicht aus. Sie werden für eine Verwertbarkeit als Prüfungsnachweis mit einer oder mehreren zusätzlichen Arten von Prüfungshandlungen kombiniert. Eigene Beobachtungen sind i.d.R. aussagekräftiger als die Verwertung von Aussagen Dritter. Allerdings beziehen sich solche Beobachtungsergebnisse immer nur auf den Zeitpunkt der Prüfung. In diesen Fällen kann es daher erforderlich sein, weitere Prüfungshandlungen in Erwägung zu ziehen, um die kontinuierliche Anwendung der Regelungen des CMS zu prüfen.

A54 Die Prüfung der Angemessenheit und Wirksamkeit der Regelungen zur Compliance-Kultur kann sich sowohl auf die Durchsicht von Regelwerken (z.B. Verhaltenskodex) und dokumentierten Verhaltensgrundsätzen, die Befragung von gesetzlichen Vertretern und Mitarbeitern bzw. Mitgliedern des Aufsichtsorgans als auch auf die Beobachtung und das Nachvollziehen des gelebten Verhaltens der Unternehmensmitglieder beziehen. In diesem Zusammenhang ist nicht nur das formale Bestehen von Regelungen, sondern insb. auch deren tatsächliche Umsetzung im Unternehmen relevant.

A55 Bei der Prüfung Angemessenheit und Wirksamkeit der Regelungen zu den Compliance-Zielen und der Compliance-Risiken kann z.B. durch Befragungen und die Durchsicht von Berichten oder Auswertungen des Unternehmens zur Zielerreichung bzw. -abweichung festgestellt werden, wie das Unternehmen die Compliance-Ziele und die einzuhaltenden Regeln bestimmt und gewichtet hat und ob geeignete Regelungen zur rechtzeitigen Risikoidentifikation für die identifizierten Risikobereiche existieren sowie ob diese kontinuierlich durch das Unternehmen

[22] Vgl. ISA [DE] 500 Prüfungsnachweise, Tz. A20.

angewendet werden. Hierbei ist auch von Bedeutung, ob die vom Unternehmen festgelegten Ziele verständlich formuliert, konsistent zueinander sind und der Grad der Zielerreichung messbar ist.

Das erlangte Verständnis von dem Unternehmen und seinem Umfeld sowie von dem zu prüfenden CMS spielt eine wichtige Rolle bei der Prüfung der Vollständigkeit der Risikoidentifikation durch den CMS-Prüfer. Relevante Fragestellungen bei der Prüfung der Regelungen zu den Compliance-Risiken können z.B. sein:

- Wie erfolgt die Risikoidentifikation und -beurteilung für den zu prüfenden Teilbereich (insb. eingesetzte Verfahren, Berücksichtigung von Interdependenzen)? Werden die einzuhaltenden Regeln hierbei angemessen berücksichtigt?
- Wer ist verantwortlich für die Risikoanalyse?
- Welche Prozesse oder Methoden gibt es, um Veränderungen an Prozessen oder Faktoren zu erkennen, die einen Einfluss auf Compliance-Risiken haben?
- Wann erfolgt eine Neueinschätzung von Compliance-Risiken?
- Welche Regelverstöße haben in der Vergangenheit zu Verlusten (z.B. als Bußgelder) geführt und welche Maßnahmen hat das Unternehmen ergriffen, um derartige Fälle in der Folge zu vermeiden?

A56 Die Prüfung des Compliance-Programms umfasst insb. die Beurteilung der Angemessenheit und Wirksamkeit der Regelungen, die vom Unternehmen zur Verhinderung oder Begrenzung der Compliance-Risiken eingerichtet wurden und auf ein regelkonformes Verhalten abzielen. Dazu gehört u.a., dass der CMS-Prüfer die Richtlinien, Arbeitsanweisungen, Handbücher oder Kontrollbeschreibungen, die zu einem regelkonformen Verhalten beitragen sollen, durchsieht und ggf. Kontrollen nachvollzieht.

Relevante Fragestellungen bei der Prüfung des Compliance-Programms können z.B. sein:

- Wie stellt das Compliance-Programm regelkonformes Verhalten sicher? Werden die identifizierten Compliance-Risiken hierbei angemessen adressiert und z.B. mittels einer „Risiko-Kontroll-Matrix“ gegenübergestellt?
- Bestehen interne Grundsätze, mit denen Mitarbeiter zu regelkonformem Verhalten angehalten werden, mit Angabe der wesentlichen Regelungsinhalte (soweit nicht selbsterklärend)?
- Welche wesentlichen Maßnahmen (Prozesse, Richtlinien, Kontrollen) zur Prävention von Regelverstößen in Bezug auf die wesentlichen identifizierten Compliance-Risiken für den zu prüfenden Teilbereich (z.B. Berechtigungskonzepte, Genehmigungsverfahren, Funktionstrennungen) sind implementiert und werden diese beachtet?

A57 Die Prüfung der Angemessenheit und Wirksamkeit der Regelungen der *Compliance-Organisation* kann z.B. die Befragung geeigneter Mitarbeiter und Nachvollzug der Regelungen dahingehend umfassen, ob die Verantwortungsbereiche und Rollen im CMS klar geregelt, abgegrenzt, kommuniziert und dokumentiert sind. Hierzu gehört auch, ob die Aufgabenträger die erforderlichen persönlichen und fachlichen Voraussetzungen erfüllen, ausreichende Ressourcen (insb. Personen, Technologie, Hilfsmittel) zur Verfügung stehen und die wesentlichen Regelungen zur Aufbau- und Ablauforganisation dokumentiert und verbindlich vorgegeben sind.

A58 Die Prüfung der Angemessenheit und Wirksamkeit der Regelungen zur *Compliance-Kommunikation* umfasst z.B. die Beurteilung, ob die entsprechenden aufbau- und ablauforganisatorischen Vorkehrungen im Unternehmen so getroffen wurden, dass die jeweils betroffenen Mitarbeiter und ggf. Dritte über die Compliance-Kultur, das Compliance-Programm sowie die festgelegten Rollen und Verantwortlichkeiten informiert werden. Zur Prüfung der Regelungen der Compliance-Kommunikation gehört zudem auch die Beurteilung, ob die Compliance-Risiken sowie Hinweise auf mögliche und festgestellte Regelverstöße an die zuständigen Stellen im Unternehmen (z.B. die gesetzlichen Vertreter und erforderlichenfalls das Aufsichtsorgan) zeitgerecht berichtet werden. Zu diesem Zweck können z.B. die Kommunikationswege und -prozesse im üblichen Geschäftsreporting sowie im Risikoreporting analysiert werden. Hierbei ist insb. von Bedeutung, ob geeignete Eskalationskriterien für die Risikokommunikation festgelegt sind, die Berichtsperiodizitäten der Bedeutung des jeweiligen Compliance-Risikos angemessen sind und ob geeignete Regelungen hinsichtlich einer ggf. erforderlichen Ad-hoc-Berichterstattung existieren.

A59 Die Prüfung der Angemessenheit und Wirksamkeit der Regelungen zur *Überwachung und Verbesserung* des CMS umfasst z.B. die Beurteilung, ob die personelle und qualitative Ausstattung der Internen Revision ausreichend ist und die ihr zugewiesenen Aufgaben zur Überwachung des CMS angemessen sind (vgl. Tz. 70 f.). Von Bedeutung kann daher die Analyse des Prüfprogramms der Internen Revision daraufhin sein, ob und inwieweit Aspekte der CMS-Überwachung Berücksichtigung fanden. Schließlich umfasst die Prüfung auch die Beurteilung der integrierten Kontrollen und sonstigen Maßnahmen (Managementkontrollen) zur Überwachung des CMS, um ein Gesamtbild von den Überwachungsprozessen zu gewinnen und hierauf basierend deren Wirksamkeit zu beurteilen.

A60 Art, Umfang und Zeitpunkt der im Rahmen der Prüfung der Angemessenheit und Wirksamkeit durchzuführenden Prüfungshandlungen sind u.a. abhängig von

- den angewandten CMS-Grundsätzen,
- den Inhalten der CMS-Beschreibung,
- den bisherigen Erfahrungen des Prüfers mit dem Unternehmen,
- den Ergebnissen der Risikobeurteilungen,
- der Ausgestaltung des CMS und dessen Dokumentation,
- der verwendeten IT-Unterstützung,
- der Art und Weise der Überwachung des CMS, z.B. durch die Interne Revision oder andere unternehmensinterne Funktionen, sowie
- Wesentlichkeitsüberlegungen.

Festgestellte Regelverstöße [Tz. 63 f.]

A61 Stellt der CMS-Prüfer einen Regelverstoß fest, der auf einen Mangel im CMS zurückzuführen sein kann (vgl. Tz. 64), wird er durch weitere Prüfungshandlungen klären, ob es sich um einen Einzelverstoß handelt, der die Angemessenheit und Wirksamkeit des CMS nicht berührt, oder ob ein Mangel im CMS vorliegt. Als Prüfungshandlungen kommen hierbei u.a. in Betracht:

- Befragungen des Managements zur eigenen Einschätzung der Ursache des festgestellten Regelverstoßes auf Basis einer Ursachenanalyse.

- Würdigung des Umgangs des Unternehmens mit dem festgestellten Regelverstoß (z.B. Unterrichtung der Mitarbeiter, Sanktionen und Anpassung der Regelungen im CMS).
- Prüfung, ob die interne Revision vergleichbare Regelverstöße identifiziert hat und welche Maßnahmen daraufhin veranlasst wurden.

Nutzung der Arbeit von Sachverständigen des Prüfers [Tz. 65 ff.]

A62 Eine Nutzung der Arbeit von Sachverständigen des Prüfers kann z.B. geboten sein bei

- der Frage der Angemessenheit des CMS, um die Beachtung spezieller Rechtsvorschriften zu untersuchen,
- der Interpretation spezifischer Anforderungen der angewandten CMS-Grundsätze,
- der Würdigung von IT-gestützten Bestandteilen des CMS sowie
- der Würdigung von Sachverhalten, die auf einen Regelverstoß hindeuten, und der Würdigung von festgestellten Regelverstößen.

A63 Informationen zu Kompetenz, Fähigkeiten und Objektivität eines Sachverständigen (vgl. Tz. 67) können aus unterschiedlichen Quellen stammen, bspw. aus

- persönlicher Erfahrung mit der bisherigen Tätigkeit des Sachverständigen,
- Gesprächen mit dem Sachverständigen,
- Gesprächen mit anderen Wirtschaftsprüfern oder anderen Personen, die mit der Arbeit des Sachverständigen vertraut sind,
- Kenntnissen über die Qualifikationen des Sachverständigen (Feststellung einer Berufszulassung bzw. Mitgliedschaft in einer Berufs- oder Branchenorganisation),
- Publikationen des Sachverständigen.

A64 Die folgenden Aspekte können bei der Beurteilung der Arbeiten externer Sachverständiger (vgl. Tz. 67) für die Zwecke des CMS-Prüfers relevant sein:

- Die Relevanz und Vertretbarkeit der Feststellungen und Schlussfolgerungen des Sachverständigen und ob diese mit anderen Prüfungsnachweisen im Einklang stehen;
- wenn den Arbeiten des Sachverständigen bedeutsame Annahmen und Methoden zugrunde liegen, die Relevanz, Vollständigkeit und Vertretbarkeit dieser Annahmen und Methoden unter den gegebenen Umständen und
- wenn die Tätigkeit des Sachverständigen in der Verwendung von Ausgangsdaten besteht, die Relevanz, Vollständigkeit und Richtigkeit dieser Ausgangsdaten.

A65 Die Beurteilung der Arbeit von externen Sachverständigen kann z.B. durch Befragungen oder die Durchsicht der Berichterstattung bzw. der Arbeitspapiere des externen Sachverständigen erfolgen.

Nutzung der Arbeit anderer Prüfer sowie Nutzung der Arbeit von Sachverständigen der gesetzlichen Vertreter und der Internen Revision [Tz. 68 ff.]

A66 Die in Tz. A62 ff. dargestellten Anwendungshinweise können sinngemäß auch auf die Nutzung der Arbeit eines anderen Prüfers bzw. auf die Nutzung der Arbeit von Sachverständigen der

gesetzlichen Vertreter und auf die Nutzung der Arbeit der Internen Revision angewandt werden.

A67 Bei der Beurteilung der Arbeit der Internen Revision ist auch relevant, inwieweit die Anforderungen aus den Internationalen Grundlagen für die berufliche Praxis der Internen Revision (IPPF) des IIA (The Institute of Internal Auditors)[23] sowie der DIIR Revisionsstandards durch die Interne Revision beachtet wurden.

Ereignisse nach dem Beurteilungszeitpunkt bzw. -zeitraum [Tz. 72 ff.]

A68 Als Prüfungshandlungen zur Feststellung von Ereignissen nach dem in der CMS-Beschreibung genannten Zeitpunkt bzw. Zeitraum, auf den sich die Darstellungen der gesetzlichen Vertreter beziehen (vgl. Tz. 72), kommen z.B. in Betracht:

- Lesen von Protokollen über in diesem Zeitraum stattgefundene Sitzungen der Verwaltungsorgane,
- Lesen von unternehmensinternen Berichten, wie z.B. Berichte der Internen Revision, sowie
- Befragungen des Compliance-Beauftragten und erforderlichenfalls der gesetzlichen Vertreter und der für die Überwachung Verantwortlichen. Die Befragungen können sich bspw. auf bis zum Zeitpunkt der Berichterstattung über die CMS-Prüfung aufgedeckte oder vermutete Regelverstöße beziehen, die die Angemessenheit und Wirksamkeit des CMS in Frage stellen.

A69 Für den Fall, dass keine Änderung der CMS-Beschreibung (vgl. Tz. 74) erfolgt, kann es erforderlich sein, die Adressaten der Berichterstattung hierüber zu informieren.

Sonstige Informationen in der CMS-Beschreibung [Tz. 76 ff.]

A70 Sonstige Informationen in einer CMS-Beschreibung, die nicht Gegenstand der Prüfung sind (vgl. Tz. 76), können z.B. Angaben zur Wirksamkeit des CMS bei einer Angemessenheitsprüfung sein. Auch können sonstige Informationen vorliegen, wenn die von den gesetzlichen Vertretern vorgelegte CMS-Beschreibung für den zu prüfenden Teilbereich Teil einer übergeordneten CMS-Beschreibung für das gesamte CMS ist. Insbesondere in diesem Fall muss nach Tz. 70 eindeutig erkennbar sein, welche Darstellungen der CMS-Beschreibung Gegenstand der Prüfung sind, damit sich keine Irreführung der Berichtsadressaten ergibt.

A71 Als weitere angemessene Maßnahme kann der CMS-Prüfer z.B. einen Hinweis (vgl. Tz. 93) in den CMS-Prüfungsbericht aufnehmen und darin die wesentliche Unstimmigkeit bzw. den wesentlichen Fehler erläutern.

[23] The Institute of Internal Auditors (IIA): Weltweite Organisation der nationalen Berufsverbände für Interne Revision.

Schriftliche Erklärungen [Tz. 80 ff.]

A72 Schriftliche Erklärungen sind kein Ersatz für andere nach diesem *IDW Prüfungsstandard* vorgesehene Prüfungshandlungen.

Auswertung der Prüfungsfeststellungen und Bildung des Prüfungsurteils [Tz. 85 ff.]

A73 Stellt der CMS-Prüfer eine Abweichung von den in der CMS-Beschreibung dargestellten Regelungen des CMS fest, wird er i.d.R. durch weitere Prüfungshandlungen klären, ob es sich um einen Einzelfall handelt, der die Angemessenheit und Wirksamkeit des CMS nicht berührt, oder ob ein Mangel im CMS vorliegt. Als Prüfungshandlungen kommen hierbei bspw. in Betracht:

- Befragung der gesetzlichen Vertreter zur eigenen Einschätzung der Ursache der festgestellten Abweichung,
- Würdigung des Umgangs des Unternehmens mit der festgestellten Abweichung und
- Prüfung, ob mit der Überwachung des CMS beauftragte Personen vergleichbare Abweichungen identifiziert haben und welche Maßnahmen daraufhin veranlasst wurden.

Dokumentation [Tz. 94 ff.]

A74 Durch die Arbeitspapiere kann gleichzeitig nachgewiesen werden, dass die CMS-Prüfung in Übereinstimmung mit diesem *IDW Prüfungsstandard* geplant und durchgeführt wurde.

CMS-Prüfungsbericht [Tz. 102 ff.]

A75 Der CMS-Prüfer erstellt den Prüfungsbericht auf der Grundlage des mit dem Unternehmen geschlossenen Auftrags. Die Prüfung des CMS wird für Zwecke des Unternehmens durchgeführt und der Prüfungsbericht ist zur Information des Unternehmens über das Ergebnis der Prüfung bestimmt. Es liegt in der Entscheidung des Unternehmens, ob der Prüfungsbericht in Abstimmung mit dem Prüfer Dritten zugänglich gemacht wird.

Weitere Berichtspflichten [Tz. 109 f.]

A76 Die Feststellung von Regelverstößen, die sich nicht auf das Prüfungsurteil auswirken, ist grundsätzlich nicht Gegenstand der CMS-Prüfung i.S. dieses *IDW Prüfungsstandards*. Im Zusammenhang mit der CMS-Prüfung kann sich jedoch für den CMS-Prüfer aus der Treuepflicht eine Pflicht zur Information des Auftraggebers ergeben, soweit anlässlich der CMS-Prüfung solche Regelverstöße festgestellt werden.

Anlagen

Anlage 1: Allgemein anerkannte CMS-Rahmenkonzepte

Name	Organisation	Anwendungsbereich
Compliance-Managementsysteme – Anforderungen mit Anleitung zur Anwendung (ISO 37301:2021)[24]	International Organization for Standardization, Genf, Schweiz	ISO 37301 legt Anforderungen fest und bietet Anleitungen für den Aufbau, die Entwicklung, die Implementierung, die Bewertung, die Instandhaltung und die Verbesserung eines effektiven Compliance-Managementsystems innerhalb einer Organisation.
Managementsysteme zur Korruptionsbekämpfung – Anforderungen mit Leitlinien zur Anwendung (ISO 37001:2016)[25]	International Organization for Standardization, Genf, Schweiz	ISO 37001 legt Anforderungen fest und gibt Leitlinien für den Aufbau, Aufrechterhaltung, Überprüfung und Verbesserung eines Managementsystems zur Korruptionsbekämpfung.
Hinweismanagementsysteme – Leitlinien (ISO/DIS 37002:2021)[26]	International Organization for Standardization, Genf, Schweiz	ISO/DIS 37002 bietet Anleitung für den Aufbau, die Verwirklichung, Aufrechterhaltung eines wirksamen, responsiven Hinweismanagementsystems.
Pflichtenheft zum Compliance Management in der Immobilienwirtschaft[27]	Initiative Corporate Governance der deutschen Immobilienwirtschaft e.V., Berlin	Grundsätze für eine transparente und professionelle Unternehmensführung in der Immobilienwirtschaft
United States Federal Sentencing Guidelines Manual[28]	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
BME-Verhaltensrichtlinie Code of Conduct[29]	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.

[24] https://www.iso.org/standard/75080.html (letzter Aufruf: 19.11.2021).

[25] https://www.beuth.de/de/norm/din-iso-37001/286423800 (letzter Aufruf: 19.11.2021).

[26] https://www.beuth.de/de/norm/iso-37002/344186348(letzter Aufruf: 19.11.2021).

[27] https://icg-institut.de/wp-content/uploads/2020/07/Pflichtenheft_2018_low.pdf (letzter Aufruf: 19.11.2021).

[28] https://www.ussc.gov/guidelines/2016-guidelines-manual (letzter Aufruf: 19.11.2021).

[29] https://www.bme.de/fileadmin/_horusdam/2065-BME-Code_of_Conduct_deutsch.pdf (letzter Aufruf: 19.11.2021).

Name	Organisation	Anwendungsbereich
The Bribery Act Guidance about procedures which relevant commercial organisations can put into place to prevent persons associated with them from bribing[30] (Guidance to the UK Bribery Act[31])	The Ministry of Justice, London	Zum „UK Bribery Act“ wurden Richtlinien veröffentlicht, die den Unternehmen helfen sollen, die Anforderungen des UK Bribery Act zu erfüllen. Der „UK Bribery Act“ ist ein Antikorruptionsgesetz, das Bestechungstaten unter Strafe stellt. Auch deutsche Unternehmen können in den Anwendungsbereich des Gesetzes fallen, wenn sie einen hinreichenden Geschäftsbezug zu Großbritannien (z.B. durch eine Betriebsstätte oder umfangreiche Warenlieferungen) haben.
Evaluation of Corporate Compliance Programs[32]	US-Justizministerium „Criminal Division of the U.S. Department of Justice“ (DoJ), Washington, USA	Der vom US-Justizministeriums veröffentlichte Leitfaden befasst sich mit der Bewertung der Angemessenheit und Wirksamkeit eines Compliance-Programms im Zuge von behördlichen Untersuchungen.

30 https://www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf (letzter Aufruf: 19.11.2021).

31 http://www.legislation.gov.uk/ukpga/2010/23/contents (letzter Aufruf: 19.11.2021).

32 https://www.justice.gov/criminal-fraud/page/file/937501/download (letzter Aufruf: 19.11.2021).

Anlage 2: Hinweise und Hilfestellungen zur Ausgestaltung von CMS

Name	Organisation	Anwendungsbereich
Das ICC Toolkit zur kartellrechtlichen Compliance[33]	ICC Germany e. V., Internationale Handelskammer, Berlin	Das Toolkit unterstützt Unternehmen bei der Implementierung und Weiterentwicklung kartellrechtlicher Compliance-Programme.
Compliance matters – What companies can do better to respect EU competition rules[34]	EU-Kommission, Brüssel	Eckpunkte einer wirksamen Compliance-Strategie zur Vermeidung von Verstößen gegen das europäische Kartell- und Marktmachtmissbrauchsverbot.
DICO Standards und Leitlinien[35]	Deutsches Institut für Compliance e.V., Berlin	DICO hat zu ausgewählten Compliance Themen Standards und Leitlinien veröffentlicht.
KICG-Leitlinien[36]	KICG – Konstanz Institut für Corporate Governance	Leitlinien mit Empfehlungen für die Ausgestaltung und Beurteilung von Compliance-Management-Systemen

[33] https://iccwbo.org/content/uploads/sites/3/2014/10/ICC-Antitrust-Compliance-Toolkit-GERMAN.pdf (letzter Aufruf: 19.11.2021).

[34] https://ec.europa.eu/competition/antitrust/compliance/index_en.html (letzter Aufruf: 19.11.2021).

[35] https://www.dico-ev.de/publikationen/ (letzter Aufruf: 19.11.2021).

[36] KICG-Leitlinien - HTWG (https://www.htwg-konstanz.de/forschung-und-transfer/institute-und-labore/kicg/publikationen/forschungsergebnisse-kicg/kicg-leitlinien/) (letzter Aufruf: 19.11.2021).

Anlage 3: Berichterstattung über CMS-Prüfungen

Formulierungsbeispiele für CMS-Prüfungsberichte

3.1. Wirksamkeitsprüfung mit uneingeschränktem Prüfungsurteil

BERICHT DES UNABHÄNGIGEN WIRTSCHAFTSPRÜFERS

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

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 sowie der Angemessenheit, Implementierung und Wirksamkeit des in der CMS-Beschreibung dargestellten Compliance Management Systems für ... [Beschreibung des oder der zu prüfenden abgegrenzten Teilbereiche(s) des CMS] durchzuführen.

Unter einem Compliance Management System (CMS) ist die Gesamtheit aller Grundsätze, Verfahren und Maßnahmen (im Folgenden zusammenfassend: Regelungen) des Unternehmens zu verstehen, die auf ein regelkonformes Verhalten des Unternehmens und seiner Mitarbeiter sowie ggf. Dritter abzielen, d.h. auf die Einhaltung bestimmter Regeln und damit auf die Verhinderung von wesentlichen Regelverstößen in abgegrenzten Teilbereichen.

Für die Durchführung des Auftrags und für unsere Verantwortlichkeit sind, auch im Verhältnis zu Dritten, die diesem Bericht beigefügten Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 01.01.2017 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 diesen Bericht auf Grundlage des mit der ... [Gesellschaft] geschlossenen Auftrags, dem, auch mit Wirkung gegenüber Dritten, die beiliegenden Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 01.01.2017 mit der Maßgabe zugrunde liegen, dass die darin enthaltenen Haftungshöchstgrenzen allen Personen gegenüber, die diese Berichterstattung mit unserer vorherigen Zustimmung erhalten haben, gemeinschaftlich bestehen.*]

B. Gegenstand, Art und Umfang der Prüfung

Gegenstand unserer Prüfung waren die in der als Anlage 1 beigefügten CMS-Beschreibung enthaltenen Darstellungen über ... [Beschreibung des oder der zu prüfenden abgegrenzten Teilbereiche(s) des CMS]. Bei der Einrichtung des CMS wurden [Bezeichnung der angewandten CMS-Grundsätze] zugrunde gelegt.

Die gesetzlichen Vertreter der [Gesellschaft] sind für das CMS einschließlich der Abgrenzung der zu prüfenden Teilbereiche und der Dokumentation des CMS sowie für die Inhalte der CMS-Beschreibung verantwortlich. Ferner sind die gesetzlichen Vertreter verantwortlich für die Prozesse und Kontrollen, die sie als notwendig erachtet haben, um die Aufstellung einer CMS-Beschreibung zu ermöglichen, die frei von wesentlichen falschen Darstellungen ist, und um ausreichende geeignete Nachweise für die Aussagen in der CMS-Beschreibung erbringen zu können.

Unsere Aufgabe ist es, auf der Grundlage der von uns durchgeführten Prüfung ein Urteil mit hinreichender Sicherheit über die angemessene Darstellung der in der CMS-Beschreibung enthaltenen Grundsätze, Verfahren und Maßnahmen (Regelungen) des CMS in Übereinstimmung mit den angewandten CMS-Grundsätzen ... [Bezeichnung der CMS-Grundsätze] abzugeben. Darüber hinaus ist es unsere Aufgabe, auf der Grundlage der von uns durchgeführten Prüfung ein Urteil mit hinreichender Sicherheit über die in der CMS-Beschreibung enthaltenen Darstellungen zur Angemessenheit, Implementierung und Wirksamkeit des ... [Beschreibung des oder der zu prüfenden abgegrenzten Teilbereiche(s) des CMS] abzugeben. Unsere Prüfung umfasst nicht die Beurteilung, welche Regelungsbereiche von den gesetzlichen Vertretern als Gegenstand der unternehmensweiten Compliance-Organisation festgelegt bzw. welche Teilbereiche als Gegenstand der CMS-Prüfung abgegrenzt wurden. Die Zielsetzung der Prüfung liegt als Systemprüfung nicht in dem Erkennen von einzelnen Regelverstößen. Sie ist daher nicht darauf ausgerichtet, Prüfungssicherheit über die tatsächliche Einhaltung von Regeln zu erlangen.

Die in der CMS-Beschreibung für ... [Beschreibung des oder der zu prüfenden abgegrenzten Teilbereiche(s) des CMS] dargestellten Regelungen des CMS sind angemessen, wenn sie geeignet sind, mit hinreichender Sicherheit sowohl Risiken für wesentliche Regelverstöße rechtzeitig zu erkennen als auch solche Regelverstöße zu verhindern. Hierzu zählt auch, dass bereits eingetretene Regelverstöße zeitnah 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 Regelungen in den laufenden Geschäftsprozessen von den hiervon betroffenen Personen nach Maßgabe ihrer Verantwortlichkeit in einem bestimmten Zeitraum wie vorgesehen eingehalten werden. Auch ein wirksames CMS unterliegt systemimmanenten Grenzen, sodass möglicherweise auch wesentliche Regelverstöße auftreten können, ohne systemseitig verhindert oder aufgedeckt zu werden.

Wir haben unsere Prüfung unter Beachtung des *Entwurfs einer Neufassung des IDW Prüfungsstandards: Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen (IDW EPS 980 n.F. (10.2021))* durchgeführt. Unsere WP-Praxis hat die Anforderungen an das Qualitätssicherungssystem des *IDW Qualitätssicherungsstandards: Anforderungen an die Qualitätssicherung in der Wirtschaftsprüferpraxis (IDW QS 1)* angewendet. Die Berufspflichten gemäß der WPO und der BS WP/vBP einschließlich der Anforderungen an die Unabhängigkeit haben wir eingehalten.

Die Prüfung ist so zu planen und durchzuführen, dass wir mit hinreichender Sicherheit beurteilen können, ob die im geprüften Zeitraum implementierten Regelungen des CMS in der CMS-Beschreibung in Übereinstimmung mit den angewandten CMS-Grundsätzen ... [Bezeichnung der CMS-Grundsätze] in allen wesentlichen Belangen angemessen dargestellt sind, ob die dargestellten Regelungen in Übereinstimmung mit den angewandten CMS-Grundsätzen ... [Bezeichnung der CMS-Grundsätze] in allen wesentlichen Belangen während des geprüften Zeitraums geeignet waren, mit hinreichender Sicherheit sowohl Risiken für wesentliche Verstöße gegen ... [Beschreibung der betreffenden Regeln bzw. des oder der abgegrenzten Teilbereiche(s)] rechtzeitig zu erkennen als auch solche Regelverstöße zu verhindern, und ob die dargestellten Regelungen in allen wesentlichen Belangen während des Zeitraums vom [Datum] bis [Datum] wirksam waren.

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 Regelungen sowie die uns vorgelegten Nachweise überwiegend auf der Basis einer Auswahl beurteilt. Wir sind der Auffassung, dass die von uns erlangten Prüfungsnachweise ausreichend und geeignet sind, um als Grundlage für unser Prüfungsurteil zu dienen.

Unser Prüfungsurteil erstreckt sich nicht auf sonstige Informationen in der CMS-Beschreibung, die nicht Gegenstand des ... [Beschreibung des oder der zu prüfenden abgegrenzten Teilbereiche(s) des CMS] sind, und dementsprechend geben wir weder ein Prüfungsurteil noch irgendeine andere Form von Prüfungsschlussfolgerung zu diesen sonstigen Informationen ab.

Im Einzelnen haben wir folgende Prüfungshandlungen durchgeführt:

[Zusammenfassende Beschreibung der Prüfungshandlungen zur Risikobeurteilung, der Angemessenheits- und Wirksamkeitsprüfungen sowie der weiteren Prüfungshandlungen]

Wir haben die Prüfung (mit Unterbrechungen) in der Zeit vom [Datum] bis [Datum] 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 des CMS schriftlich bestätigt.

C. Feststellungen zum Compliance Management System

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

[einschl. Beschreibung der angewandten CMS-Grundsätze]

Ausführungen zu den einzelnen CMS-Grundelementen:

Compliance-Kultur

Compliance-Ziele

Compliance-Risiken

Compliance-Programm

Compliance-Organisation

Compliance-Kommunikation

Compliance-Überwachung und Verbesserung.

II. Feststellungen [und Empfehlungen]

[a. Feststellungen, die zu einer Einschränkung, Versagung oder Erklärung der Nichtabgabe des Prüfungsurteils geführt haben

b. sonstige Feststellungen

c. ggf. Darstellung von bedeutenden Schwierigkeiten bei der Beurteilung des Prüfungsgegenstands

d. ggf. Empfehlungen]

D. Zusammenfassendes Prüfungsurteil

Nach unserer Beurteilung aufgrund der bei der Prüfung gewonnenen Erkenntnisse

- sind die im Zeitraum von [Datum] bis [Datum] implementierten Grundsätze, Verfahren und Maßnahmen (Regelungen) des CMS in der CMS-Beschreibung in Übereinstimmung mit den angewandten CMS-Grundsätzen ... [Bezeichnung der CMS-Grundsätze] in allen wesentlichen Belangen angemessen dargestellt,
- waren die in der CMS-Beschreibung dargestellten Regelungen in Übereinstimmung mit den angewandten CMS-Grundsätzen ... [Bezeichnung der CMS-Grundsätze] in allen wesentlichen Belangen
  - während des Zeitraums von [Datum] bis [Datum] geeignet, mit hinreichender Sicherheit sowohl Risiken für wesentliche Regelverstöße gegen ... [Beschreibung

der betreffenden Regeln bzw. des oder der zu prüfenden abgegrenzten Teilbereiche(s)] rechtzeitig zu erkennen als auch solche Regelverstöße zu verhindern, und

– während des Zeitraums vom [Datum] bis [Datum] wirksam.

Ohne unser Prüfungsurteil einzuschränken, weisen wir darauf hin, dass die CMS-Beschreibung für ... [Beschreibung des oder der zu prüfenden abgegrenzten Teilbereiche(s) des CMS] bei der Gesellschaft zum [Datum] aufgestellt wurde. Die Ausführungen zu den Prüfungshandlungen zur Beurteilung der Wirksamkeit einzelner Regelungen erstrecken sich daher auf den Zeitraum vom [Datum] bis [Datum]. Jede Übertragung dieser Angaben auf einen zukünftigen Zeitpunkt birgt die Gefahr, dass wegen zwischenzeitlicher Änderungen des CMS falsche Schlussfolgerungen gezogen werden.

[Ort]

[Datum]

[Unterschrift]

Anlagen:

[CMS-Beschreibung]

[Allgemeine Auftragsbedingungen]

3.2. Wirksamkeitsprüfung mit eingeschränktem Prüfungsurteil wegen eines Prüfungshemmnisses

BERICHT DES UNABHÄNGIGEN WIRTSCHAFTSPRÜFERS

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

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 sowie der Angemessenheit, Implementierung und Wirksamkeit des in der CMS-Beschreibung dargestellten Compliance Management Systems für ... [Beschreibung des oder der zu prüfenden abgegrenzten Teilbereiche(s) des CMS] durchzuführen.

Unter einem Compliance Management System (CMS) ist die Gesamtheit aller Grundsätze, Verfahren und Maßnahmen (im Folgenden zusammenfassend: Regelungen) des Unternehmens zu verstehen, die auf ein regelkonformes Verhalten des Unternehmens und seiner Mitarbeiter sowie ggf. Dritter abzielen, d.h. auf die Einhaltung bestimmter Regeln und damit auf die Verhinderung von wesentlichen Regelverstößen in abgegrenzten Teilbereichen.

Für die Durchführung des Auftrags und für unsere Verantwortlichkeit sind, auch im Verhältnis zu Dritten, die diesem Bericht beigefügten Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 01.01.2017 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 diesen Bericht auf Grundlage des mit der ... [Gesellschaft] geschlossenen Auftrags, dem, auch mit Wirkung gegenüber Dritten, die beiliegenden Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 01.01.2017 mit der Maßgabe zugrunde liegen, dass die darin enthaltenen Haftungshöchstgrenzen allen Personen gegenüber, die diese Berichterstattung mit unserer vorherigen Zustimmung erhalten haben, gemeinschaftlich bestehen.]

B. Gegenstand, Art und Umfang der Prüfung

Gegenstand unserer Prüfung waren die in der als Anlage 1 beigefügten CMS-Beschreibung enthaltenen Darstellungen über ... [Beschreibung des oder der zu prüfenden abgegrenzten Teilbereiche(s) des CMS]. Bei der Einrichtung des CMS wurden [Bezeichnung der angewandten CMS-Grundsätze] zugrunde gelegt.

Die gesetzlichen Vertreter der [Gesellschaft] sind für das CMS einschließlich der Abgrenzung der zu prüfenden Teilbereiche und der Dokumentation des CMS sowie für die Inhalte der CMS-Beschreibung verantwortlich. Ferner sind die gesetzlichen Vertreter verantwortlich für die Prozesse und Kontrollen, die sie als notwendig erachtet haben, um die Aufstellung einer CMS-Beschreibung zu ermöglichen, die frei von wesentlichen falschen Darstellungen ist, und um ausreichende geeignete Nachweise für die Aussagen in der CMS-Beschreibung erbringen zu können.

Unsere Aufgabe ist es, auf der Grundlage der von uns durchgeführten Prüfung ein Urteil mit hinreichender Sicherheit über die angemessene Darstellung der in der CMS-Beschreibung enthaltenen Grundsätze, Verfahren und Maßnahmen (Regelungen) des CMS in Übereinstimmung mit den angewandten CMS-Grundsätzen ... [Bezeichnung der CMS-Grundsätze] abzugeben. Darüber hinaus ist es unsere Aufgabe, auf der Grundlage der von uns durchgeführten Prüfung ein Urteil mit hinreichender Sicherheit über die in der CMS-Beschreibung enthaltenen Darstellungen zur Angemessenheit, Implementierung und Wirksamkeit des ... [Beschreibung des oder der zu prüfenden abgegrenzten Teilbereiche(s) des CMS] abzugeben. Unsere Prüfung umfasst nicht die Beurteilung, welche Regelungsbereiche von den gesetzlichen Vertretern als Gegenstand der unternehmensweiten Compliance-Organisation festgelegt bzw. welche Teilbereiche als Gegenstand der CMS-Prüfung abgegrenzt wurden. Die Zielsetzung der Prüfung liegt als Systemprüfung auch nicht in dem Erkennen von einzelnen Regelverstößen. Sie ist daher nicht darauf ausgerichtet, Prüfungssicherheit über die tatsächliche Einhaltung von Regeln zu erlangen.

Die in der CMS-Beschreibung für ... [Beschreibung des oder der zu prüfenden abgegrenzten Teilbereiche(s) des CMS] dargestellten Regelungen des CMS sind angemessen, wenn sie geeignet sind, mit hinreichender Sicherheit sowohl Risiken für wesentliche Regelverstöße rechtzeitig zu erkennen als auch solche Regelverstöße zu verhindern. Hierzu zählt auch, dass bereits eingetretene Regelverstöße zeitnah 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 Regelungen in den laufenden Geschäftsprozessen von den hiervon betroffenen Personen nach Maßgabe ihrer Verantwortlichkeit in einem bestimmten Zeitraum wie vorgesehen eingehalten werden. Auch ein wirksames CMS unterliegt systemimmanenten Grenzen, sodass möglicherweise auch wesentliche Regelverstöße auftreten können, ohne systemseitig verhindert oder aufgedeckt zu werden.

Wir haben unsere Prüfung unter Beachtung des *Entwurfs einer Neufassung des IDW Prüfungsstandards: Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen (IDW EPS 980 n.F. (10.2021))* durchgeführt. Unsere WP-Praxis hat die Anforderungen an das Qualitätssicherungssystem des *IDW Qualitätssicherungsstandards: Anforderungen an die Qualitätssicherung in der Wirtschaftsprüferpraxis (IDW QS 1)* angewendet. Die Berufspflichten gemäß der WPO und der BS WP/vBP einschließlich der Anforderungen an die Unabhängigkeit haben wir eingehalten.

Die Prüfung ist so zu planen und durchzuführen, dass wir mit hinreichender Sicherheit beurteilen können, ob die im geprüften Zeitraum implementierten Regelungen des CMS in der CMS-Beschreibung in Übereinstimmung mit den angewandten CMS-Grundsätzen ... [Bezeichnung der CMS-Grundsätze] in allen wesentlichen Belangen angemessen dargestellt sind, ob die dargestellten Regelungen in Übereinstimmung mit den angewandten CMS-Grundsätzen … [Bezeichnung der CMS-Grundsätze] in allen wesentlichen Belangen während des geprüften Zeitraums geeignet waren, mit hinreichender Sicherheit sowohl Risiken für wesentliche Verstöße gegen ... [Beschreibung der betreffenden Regeln bzw. des oder der abgegrenzten Teilbereiche(s)] rechtzeitig zu erkennen als auch solche Regelverstöße zu verhindern, und ob die dargestellten Regelungen in allen wesentlichen Belangen während des Zeitraums vom [Datum] bis [Datum] wirksam waren.

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 Regelungen sowie die uns vorgelegten Nachweise überwiegend auf der Basis einer Auswahl beurteilt. Wir sind der Auffassung, dass die von uns erlangten Prüfungsnachweise ausreichend und geeignet sind, um als Grundlage für unser Prüfungsurteil zu dienen.

Unser Prüfungsurteil erstreckt sich nicht auf sonstige Informationen in der CMS-Beschreibung, die nicht Gegenstand des ... [Beschreibung des oder der zu prüfenden abgegrenzten Teilbereiche(s) des CMS] sind, und dementsprechend geben wir weder ein Prüfungsurteil noch irgendeine andere Form von Prüfungsschlussfolgerung zu diesen sonstigen Informationen ab.

Im Einzelnen haben wir folgende Prüfungshandlungen durchgeführt:

[Zusammenfassende Beschreibung der Prüfungshandlungen zur Risikobeurteilung, der Angemessenheits- und Wirksamkeitsprüfung sowie der weiteren Prüfungshandlungen]

Wir haben die Prüfung (mit Unterbrechungen) in der Zeit vom [Datum] bis [Datum] 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 des CMS schriftlich bestätigt.

C. Feststellungen zum Compliance Management System

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

[einschl. Beschreibung der angewandten CMS-Grundsätze]

Ausführungen zu den einzelnen CMS-Grundelementen:

Compliance-Kultur

Compliance-Ziele

Compliance-Risiken

Compliance-Programm

Compliance-Organisation

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 Regelungen für ... [Beschreibung des betreffenden Bereichs] erhalten haben, können wir die Angemessenheit und Wirksamkeit dieser Regelungen nicht beurteilen. Es kann daher nicht ausgeschlossen werden, dass das CMS insoweit nicht geeignet ist, mit hinreichender Sicherheit sowohl Risiken für wesentliche Regelverstöße rechtzeitig zu erkennen als auch solche Regelverstöße zu verhindern.]

[b. sonstige Feststellungen

c. ggf. Darstellung von bedeutenden Schwierigkeiten bei der Beurteilung des Prüfungsgegenstands

d. Empfehlungen]

D. Zusammenfassendes Prüfungsurteil

Mit Ausnahme der unter C.II. erläuterten Einschränkung sind nach unserer Beurteilung aufgrund der bei der Prüfung gewonnenen Erkenntnisse

- die im Zeitraum von [Datum] bis [Datum] implementierten Grundsätze, Verfahren und Maßnahmen (Regelungen) des CMS in der CMS-Beschreibung in Übereinstimmung mit den angewandten CMS-Grundsätzen ... [Bezeichnung der CMS-Grundsätze] in allen wesentlichen Belangen angemessen dargestellt,
- waren die in der CMS-Beschreibung dargestellten Regelungen in Übereinstimmung mit den angewandten CMS-Grundsätzen ... [Bezeichnung der CMS-Grundsätze] in allen wesentlichen Belangen
  - während des Zeitraums von [Datum] bis [Datum] geeignet, mit hinreichender Sicherheit sowohl Risiken für wesentliche Regelverstöße gegen ... [Beschreibung der betreffenden Regeln bzw. des oder der zu prüfenden abgegrenzten Teilbereiche(s)] rechtzeitig zu erkennen als auch solche Regelverstöße zu verhindern, und
  - während des Zeitraums vom [Datum] bis [Datum] wirksam.

Ohne unser Prüfungsurteil darüber hinaus einzuschränken, weisen wir darauf hin, dass die CMS-Beschreibung für ... [Beschreibung des oder der zu prüfenden abgegrenzten Teilbereiche(s) des CMS] bei der Gesellschaft zum [Datum] aufgestellt wurde. Die Ausführungen zu den Prüfungshandlungen zur Beurteilung der Wirksamkeit einzelner Regelungen erstrecken sich daher auf den Zeitraum vom [Datum] bis [Datum]. Jede Übertragung dieser Angaben auf einen zukünftigen Zeitpunkt birgt die Gefahr, dass wegen zwischenzeitlicher Änderungen des CMS falsche Schlussfolgerungen gezogen werden.

[Ort]

[Datum]

[Unterschrift]

Anlagen:

[CMS-Beschreibung]

[Allgemeine Auftragsbedingungen]

3.3. Angemessenheitsprüfung mit uneingeschränktem Prüfungsurteil

BERICHT DES UNABHÄNGIGEN WIRTSCHAFTSPRÜFERS

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

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 sowie der Angemessenheit und Implementierung des in der CMS-Beschreibung dargestellten Compliance Management Systems für ... [Beschreibung des oder der zu prüfenden abgegrenzten Teilbereiche(s) des CMS] durchzuführen.

Unter einem Compliance Management System (CMS) ist die Gesamtheit aller Grundsätze, Verfahren und Maßnahmen (im Folgenden zusammenfassend: Regelungen) des Unternehmens zu verstehen, die auf ein regelkonformes Verhalten des Unternehmens und seiner Mitarbeiter sowie ggf. Dritter abzielen, d.h. auf die Einhaltung bestimmter Regeln und damit auf die Verhinderung von wesentlichen Regelverstößen in abgegrenzten Teilbereichen.

Für die Durchführung des Auftrags und für unsere Verantwortlichkeit sind, auch im Verhältnis zu Dritten, die diesem Bericht beigefügten Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 01.01.2017 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 diesen Bericht auf Grundlage des mit der ... [Gesellschaft] geschlossenen Auftrags, dem, auch mit Wirkung gegenüber Dritten, die beiliegenden Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 01.01.2017 mit der Maßgabe zugrunde liegen, dass die darin enthaltenen Haftungshöchstgrenzen allen Personen gegenüber, die diese Berichterstattung mit unserer vorherigen Zustimmung erhalten haben, gemeinschaftlich bestehen.]

B. Gegenstand, Art und Umfang der Prüfung

Gegenstand unserer Prüfung waren die in der als Anlage 1 beigefügten CMS-Beschreibung enthaltenen Darstellungen über ... [Beschreibung des oder der zu prüfenden abgegrenzten Teilbereiche(s) des CMS]. Bei der Einrichtung des CMS wurden [Bezeichnung der angewandten CMS-Grundsätze] zugrunde gelegt.

Die gesetzlichen Vertreter der [Gesellschaft] sind für das CMS einschließlich der Abgrenzung der zu prüfenden Teilbereiche und der Dokumentation des CMS sowie für die Inhalte der CMS-Beschreibung verantwortlich. Ferner sind die gesetzlichen Vertreter verantwortlich für die Prozesse und Kontrollen, die sie als notwendig erachtet haben, um die Aufstellung einer CMS-Beschreibung zu ermöglichen, die frei von wesentlichen falschen Darstellungen ist, und um ausreichende geeignete Nachweise für die Aussagen in der CMS-Beschreibung erbringen zu können.

Unsere Aufgabe ist es, auf der Grundlage der von uns durchgeführten Prüfung ein Urteil mit hinreichender Sicherheit über die angemessene Darstellung der in der CMS-Beschreibung enthaltenen Grundsätze, Verfahren und Maßnahmen (Regelungen) des CMS in Übereinstimmung mit den angewandten CMS-Grundsätzen ... [Bezeichnung der CMS-Grundsätze] abzugeben. Darüber hinaus ist es unsere Aufgabe, auf der Grundlage der von uns durchgeführten Prüfung ein Urteil mit hinreichender Sicherheit über die in der CMS-Beschreibung enthaltenen Darstellungen zur Angemessenheit und Implementierung des ... [Beschreibung des oder der zu prüfenden abgegrenzten Teilbereiche(s) des CMS] abzugeben. Unsere Prüfung umfasst nicht die Beurteilung, welche Regelungsbereiche von den gesetzlichen Vertretern als Gegenstand der unternehmensweiten Compliance-Organisation festgelegt bzw. welche Teilbereiche als Gegenstand der CMS-Prüfung abgegrenzt wurden. Die Zielsetzung der Prüfung liegt als Systemprüfung auch nicht in dem Erkennen von einzelnen Regelverstößen. Sie ist daher nicht darauf ausgerichtet, Prüfungssicherheit über die tatsächliche Einhaltung von Regeln zu erlangen.

Die in der CMS-Beschreibung für ... [Beschreibung des oder der zu prüfenden abgegrenzten Teilbereiche(s) des CMS] dargestellten Regelungen des CMS sind angemessen, wenn sie geeignet sind, mit hinreichender Sicherheit sowohl Risiken für wesentliche Regelverstöße rechtzeitig zu erkennen als auch solche Regelverstöße zu verhindern. Hierzu zählt auch, dass bereits eingetretene Regelverstöße zeitnah an die zuständige Stelle im Unternehmen zu berichten sind, damit die notwendigen Konsequenzen für eine Verbesserung des CMS getroffen werden.

Wir haben unsere Prüfung unter Beachtung des *Entwurfs einer Neufassung des IDW Prüfungsstandards: Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen (IDW EPS 980 n.F. (10.2021))* durchgeführt. Unsere WP-Praxis hat die Anforderungen an das Qualitätssicherungssystem des *IDW Qualitätssicherungsstandard: Anforderungen an die Qualitätssicherung in der Wirtschaftsprüferpraxis (IDW QS 1)* angewendet. Die Berufspflichten gemäß der WPO und der BS WP/vBP einschließlich der Anforderungen an die Unabhängigkeit haben wir eingehalten.

Die Prüfung ist so zu planen und durchzuführen, dass wir mit hinreichender Sicherheit beurteilen können, ob die zum geprüften Zeitpunkt implementierten Regelungen des CMS in der CMS-Beschreibung in Übereinstimmung mit den angewandten CMS-Grundsätzen ... [Bezeichnung der CMS-Grundsätze des CMS] in allen wesentlichen Belangen angemessen dargestellt sind, ob die dargestellten Regelungen in Übereinstimmung mit den angewandten CMS-Grundsätzen ... [Bezeichnung der CMS-Grundsätze] in allen wesentlichen Belangen geeignet waren, mit hinreichender Sicherheit sowohl Risiken für wesentliche Verstöße gegen ...

[Beschreibung der betreffenden Regeln bzw. des oder der abgegrenzten Teilbereiche(s)] rechtzeitig zu erkennen als auch solche Regelverstöße zu verhindern, und ob die dargestellten Regelungen in allen wesentlichen Belangen zum [Datum] implementiert waren.

Auftragsgemäß umfasste unsere Prüfung nicht die Beurteilung der Wirksamkeit der in der CMS-Beschreibung des Unternehmens dargestellten Regelungen.

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 Regelungen sowie die uns vorgelegten Nachweise überwiegend auf der Basis einer Auswahl beurteilt. Wir sind der Auffassung, dass die von uns erlangten Prüfungsnachweise ausreichend und geeignet sind, um als Grundlage für unser Prüfungsurteil zu dienen.

Unser Prüfungsurteil erstreckt sich nicht auf sonstige Informationen in der CMS-Beschreibung, die nicht Gegenstand des ... [Beschreibung des oder der zu prüfenden abgegrenzten Teilbereiche(s) des CMS] sind, und dementsprechend geben wir weder ein Prüfungsurteil noch irgendeine andere Form von Prüfungsschlussfolgerung zu diesen sonstigen Informationen ab.

Im Einzelnen haben wir folgende Prüfungshandlungen durchgeführt:

[Zusammenfassende Beschreibung der Prüfungshandlungen zur Risikobeurteilung, der Aufbauprüfungen sowie der weiteren Prüfungshandlungen.]

Wir haben die Prüfung (mit Unterbrechungen) in der Zeit vom [Datum] bis [Datum] 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 zu prüfenden abgegrenzten Teilbereiche(s) des CMS]

[einschl. Beschreibung der angewandten CMS-Grundsätze]

Ausführungen zu den einzelnen CMS-Grundelementen:

Compliance-Kultur

Compliance-Ziele

Compliance-Risiken

Compliance-Programm

Compliance-Organisation

Compliance-Kommunikation

Compliance-Überwachung und Verbesserung.

II. Feststellungen [und Empfehlungen]

[Feststellungen, die zu einer Einschränkung, Versagung oder Erklärung der Nichtabgabe des Prüfungsurteils geführt haben

b. sonstige Feststellungen

c. ggf. Darstellung von bedeutenden Schwierigkeiten bei der Beurteilung des Prüfungsgegenstands

d. ggf. Empfehlungen]

D. Zusammenfassendes Prüfungsurteil

Nach unserer Beurteilung aufgrund der bei der Prüfung gewonnenen Erkenntnisse

- sind die zum [Datum] implementierten Grundsätze, Verfahren und Maßnahmen (Regelungen) des CMS in der CMS-Beschreibung in Übereinstimmung mit den angewandten CMS-Grundsätzen ... [Bezeichnung der CMS-Grundsätze] in allen wesentlichen Belangen angemessen dargestellt,
- waren die in der CMS-Beschreibung dargestellten Regelungen in Übereinstimmung mit den angewandten CMS-Grundsätzen ... [Bezeichnung der CMS-Grundsätze] in allen wesentlichen Belangen
  - geeignet, mit hinreichender Sicherheit sowohl Risiken für wesentliche Regelverstöße gegen ... [Beschreibung der betreffenden Regeln bzw. des oder der zu prüfenden abgegrenzten Teilbereiche(s)] rechtzeitig zu erkennen als auch solche Regelverstöße zu verhindern, und
  - zum [Datum] implementiert.

[Ort]

[Datum]

[Unterschrift]

Anlagen:

[CMS-Beschreibung]

[Allgemeine Auftragsbedingungen]

3.4. Kurzfassung der Berichterstattung des unabhängigen Wirtschaftsprüfers bei einer Wirksamkeitsprüfung für Zwecke der Veröffentlichung

BERICHT DES UNABHÄNGIGEN WIRTSCHAFTSPRÜFERS ÜBER DIE PRÜFUNG DER ANGEMESSENHEIT, IMPLEMENTIERUNG UND WIRKSAMKEIT DES COMPLIANCE MANAGEMENT SYSTEMS FÜR … [BESCHREIBUNG DES ODER DER ZU PRÜFENDEN ABGEGRENZTEN TEILBEREICHE(S) DES CMS]

An die [Gesellschaft]

Wir haben die in Anlage 1 beigefügte CMS-Beschreibung der gesetzlichen Vertreter sowie die Angemessenheit, Implementierung und Wirksamkeit des in der CMS-Beschreibung dargestellten Compliance Management Systems für ... [Beschreibung des oder der zu prüfenden abgegrenzten Teilbereiche(s) des CMS] geprüft.

Verantwortung der gesetzlichen Vertreter

Die gesetzlichen Vertreter der [Gesellschaft] sind für das CMS einschließlich der Abgrenzung der von uns zu prüfenden Teilbereiche sowie die Dokumentation des CMS und die Inhalte der CMS-Beschreibung verantwortlich. Bei der Einrichtung des CMS wurden [Bezeichnung der angewandten CMS-Grundsätze] zugrunde gelegt. Ferner sind die gesetzlichen Vertreter verantwortlich für die Prozesse und Kontrollen, die sie als notwendig erachtet haben, um die Aufstellung einer CMS-Beschreibung zu ermöglichen, die frei von wesentlichen falschen Darstellungen ist, und um ausreichende geeignete Nachweise für die Aussagen in der CMS-Beschreibung erbringen zu können.

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

Verantwortung des Wirtschaftsprüfers

Unsere Aufgabe ist es, auf der Grundlage der von uns durchgeführten Prüfung ein Urteil mit hinreichender Sicherheit über die angemessene Darstellung der in der CMS-Beschreibung enthaltenen Grundsätze, Verfahren und Maßnahmen (Regelungen) des CMS in Übereinstimmung mit den angewandten CMS-Grundsätzen ... [Bezeichnung der CMS-Grundsätze] abzugeben. Darüber hinaus ist es unsere Aufgabe, auf der Grundlage der von uns durchgeführten Prüfung ein Urteil mit hinreichender Sicherheit über die in der CMS-Beschreibung enthaltenen Darstellungen zur Angemessenheit, Implementierung und Wirksamkeit des ... [Beschreibung des oder der zu prüfenden abgegrenzten Teilbereiche(s) des CMS] abzugeben. Unsere Prüfung umfasst nicht die Beurteilung, welche Regelungsbereiche von den gesetzlichen Vertretern als Gegenstand der unternehmensweiten Compliance-Organisation festgelegt bzw. welche Teilbereiche als Gegenstand der CMS-Prüfung abgegrenzt wurden. Die Zielsetzung der Prüfung liegt als Systemprüfung auch nicht in dem Erkennen von einzelnen Regelverstößen. Sie ist daher nicht darauf ausgerichtet, Prüfungssicherheit über die tatsächliche Einhaltung von Regeln zu erlangen.

Wir haben unsere Prüfung unter Beachtung des *Entwurfs einer Neufassung des IDW Prüfungsstandards: Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen (IDW EPS 980 n.F. (10.2021))* durchgeführt. Unsere WP-Praxis hat die Anforderungen an das Qualitätssicherungssystem des *IDW Qualitätssicherungsstandards: Anforderungen an die Qualitätssicherung in der Wirtschaftsprüferpraxis (IDW QS 1)* angewendet. Die Berufspflichten gemäß der WPO und der BS WP/vBP einschließlich der Anforderungen an die Unabhängigkeit haben wir eingehalten.

Die Prüfung ist so zu planen und durchzuführen, dass wir mit hinreichender Sicherheit beurteilen können, ob die im geprüften Zeitraum implementierten Regelungen des CMS in der CMS-Beschreibung in Übereinstimmung mit den angewandten CMS-Grundsätzen ... [Bezeichnung der CMS-Grundsätze] in allen wesentlichen Belangen angemessen dargestellt sind, ob die dargestellten Regelungen in Übereinstimmung mit den angewandten CMS-Grundsätzen ... [Bezeichnung der CMS-Grundsätze] in allen wesentlichen Belangen während des geprüften Zeitraums geeignet waren, mit hinreichender Sicherheit sowohl Risiken für wesentliche Verstöße gegen ... [Beschreibung der betreffenden Regeln bzw. des oder der abgegrenzten Teilbereiche(s)] rechtzeitig zu erkennen als auch solche Regelverstöße zu verhindern, und ob die dargestellten Regelungen in allen wesentlichen Belangen während des Zeitraums vom [Datum] bis [Datum] wirksam waren.

Die Auswahl der Prüfungshandlungen haben wir nach unserem pflichtgemäßen Ermessen vorgenommen. Wir haben die in der CMS-Beschreibung dargestellten Regelungen sowie die uns vorgelegten Nachweise überwiegend auf der Basis einer Auswahl beurteilt. Wir sind der Auffassung, dass die von uns erlangten Prüfungsnachweise ausreichend und geeignet sind, um als Grundlage für unser Prüfungsurteil zu dienen.

Unser Prüfungsurteil erstreckt sich nicht auf sonstige Informationen in der CMS-Beschreibung, die nicht Gegenstand des ... [Beschreibung des oder der zu prüfenden abgegrenzten Teilbereiche(s) des CMS] sind, und dementsprechend geben wir weder ein Prüfungsurteil noch irgendeine andere Form von Prüfungsschlussfolgerung zu diesen sonstigen Informationen ab.

Im Einzelnen haben wir folgende Prüfungshandlungen durchgeführt:

[Zusammenfassende Beschreibung der Prüfungshandlungen zur Risikobeurteilung, der Angemessenheits- und Wirksamkeitsprüfung sowie der weiteren Prüfungshandlungen]

Prüfungsurteil

Nach unserer Beurteilung aufgrund der bei der Prüfung gewonnenen Erkenntnisse

- sind die im Zeitraum von [Datum] bis [Datum] implementierten Grundsätze, Verfahren und Maßnahmen (Regelungen) des CMS in der CMS-Beschreibung in Übereinstimmung mit den angewandten CMS-Grundsätzen ... [Bezeichnung der CMS-Grundsätze] in allen wesentlichen Belangen angemessen dargestellt,

- waren die in der CMS-Beschreibung dargestellten Regelungen in Übereinstimmung mit den angewandten CMS-Grundsätzen ... [Bezeichnung der CMS-Grundsätze] in allen wesentlichen Belangen
  - während des Zeitraums von [Datum] bis [Datum] geeignet, mit hinreichender Sicherheit sowohl Risiken für wesentliche Regelverstöße gegen ... [Beschreibung der betreffenden Regeln bzw. des oder der zu prüfenden abgegrenzten Teilbereiche(s)] rechtzeitig zu erkennen als auch solche Regelverstöße zu verhindern, und
  - während des Zeitraums vom [Datum] bis [Datum] wirksam.

Ohne unser Prüfungsurteil einzuschränken, weisen wir darauf hin, dass die CMS-Beschreibung für ... [Beschreibung des oder der zu prüfenden abgegrenzten Teilbereiche(s) des CMS] bei der Gesellschaft zum [Datum] aufgestellt wurde. Die Ausführungen zu den Prüfungshandlungen zur Beurteilung der Wirksamkeit einzelner Regelungen erstrecken sich daher auf den Zeitraum vom [Datum] bis [Datum]. Jede Übertragung dieser Angaben auf einen zukünftigen Zeitpunkt birgt die Gefahr, dass wegen zwischenzeitlicher Änderungen des CMS falsche Schlussfolgerungen gezogen werden.

[Gegebenenfalls Hinweis auf sonstige Sachverhalte]

Ohne unser Prüfungsurteil einzuschränken, weisen wir darauf hin, dass [Hinweis auf sonstige Sachverhalte, wenn dies zum Verständnis des Prüfungsauftrags, der Verantwortung des Wirtschaftsprüfers oder zum Verständnis des Kurzberichts erforderlich ist.]

Auftragsbedingungen

Wir erstellen diesen Bericht auf Grundlage des mit der ... [Gesellschaft] geschlossenen Auftrags, dem, auch mit Wirkung gegenüber Dritten, die beiliegenden Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 01.01.2017 mit der Maßgabe zugrunde liegen, dass die darin enthaltenen Haftungshöchstgrenzen allen Personen gegenüber, die diese Berichterstattung mit unserer vorherigen Zustimmung erhalten haben, gemeinschaftlich bestehen.

Über Art und Umfang sowie über das Ergebnis unserer Prüfung erstatten wir einen Bericht, der ausschließlich an die [Gesellschaft] zur Verwendung [für interne Zwecke] gerichtet ist. Die Inhalte des Berichts gehen über diese Kurzfassung hinaus. Ein vollumfängliches Verständnis über unseren Auftrag, die Vorgehensweise unserer Prüfung sowie unserer Feststellungen kann regelmäßig nur durch das Lesen unseres Berichts gewonnen werden.

[Ort]

[Datum]

[Unterschrift]

Anlagen:

[CMS-Beschreibung]

[Allgemeine Auftragsbedingungen]