

CB-BEITRAG

Markus Link und Dr. Antonia Steßl

IDW EPS 981 – Erste Überlegungen zur Prüfung von Risikomanagementsystemen und seiner Bedeutung im Kontext effektiver Corporate Governance

Mit der Veröffentlichung des Entwurfs eines neuen Prüfungsstandards zur Prüfung von Risikomanagementsystemen (IDW EPS 981) wird eine weitere Grundlage geschaffen, um Unternehmensorgane in ihrer Überwachungsfunktion eines wirksamen Corporate-Governance-Systems zu unterstützen. Nachfolgend werden die Elemente dieses Standards dargestellt, die Prüfungsmöglichkeiten skizziert und in ihrer Bedeutung im Kontext der einzelnen Governance-Funktionen – insbesondere im Vergleich zum IDW PS 980, aber auch in Ausblick auf weiter geplante Standards der Governance-Elemente – sowie in Abgrenzung zu bestehenden Risikofrüherkennungssystemen – für die zukünftige weitere Entwicklung diskutiert.

I. Einleitung

Das Institut der Wirtschaftsprüfer e. V. (IDW) hat mit der Veröffentlichung des Entwurfs eines Prüfungsstandards für die Prüfung der „Grundsätze ordnungsmäßiger Prüfung von Risikomanagementsystemen (IDW EPS 981)“ am 20.2.2016 den Inhalt freiwilliger Prüfungen von Risikomanagementsystemen verdeutlicht und legt damit die Berufsauffassung dar, nach der Wirtschaftsprüfer unbeschadet ihrer Eigenverantwortlichkeit derartige Aufträge planen und durchführen sowie darüber Bericht erstatten sollen.¹ Zusammen mit dem bereits am 11.3.2011 veröffentlichten Standard zu den „Grundsätzen ordnungsmäßiger Prüfungen von Compliance Management Systemen“ (IDW PS 980) und den zu erwartenden Prüfungsstandards zur ordnungsmäßigen Prüfung der Governance-Elemente Internes Kontrollsystem und Interne Revision, hat das IDW damit ein konsistentes Set von Standards geschaffen, mit deren Hilfe der Wirtschaftsprüfer den Vorstand und Aufsichtsrat bzw. den Prüfungsausschuss hinsichtlich der straf- und haftungsrechtlichen Regeln nach §§ 130, 30, 9 OWiG sowie § 93 Abs. 1 AktG, § 107 Abs. 3 AktG unterstützen kann.

Im Rahmen des Bilanzrechtsmodernisierungsgesetzes (BilMoG) im Jahre 2009 wurde etwa über § 107 Abs. 3 S. 2 AktG bestimmt, dass sich der Aufsichtsrat bzw. der Prüfungsausschuss (soweit dieser bestellt wurde) neben der Abschlussprüfung mit der

- Überwachung des Rechnungslegungsprozesses, sowie der Wirksamkeit des
- Internen Kontrollsystems (IKS),
- des Risikomanagementsystems (RMS) und
- des internen Revisionssystems (IRS)

zu befassen hat. Dabei umfassen die Überwachungsaufgaben des Aufsichtsrats auch die Maßnahmen des Vorstands, die sich auf die

Begrenzung der Risiken aus möglichen Verstößen gegen gesetzliche Vorschriften und interne Richtlinien (Compliance) beziehen.² Diesem Sachverhalt trägt auch der Deutsche Corporate Governance Kodex (DCGK) in seiner Ziff. 5.3.2. Rechnung, nach dem sich der Aufsichtsrat „(...) insbesondere mit der Überwachung des Rechnungslegungsprozesses, der Wirksamkeit des internen Kontrollsystems, des Risikomanagementsystems und des internen Revisionssystems, (...) sowie der Compliance (...)“³ befassen soll.

Während die Befassung durch den Aufsichtsrat und den Prüfungsausschuss voraussetzt, dass die entsprechenden Systeme vorhanden sind, ist – ungeachtet der Pflichten nach § 91 Abs. 2 AktG – die Einrichtung, Ausgestaltung und Überwachung der Systeme eine im Organisationsermessen des Vorstands stehende unternehmerische Entscheidung, durch die der Vorstand vor dem Hintergrund der unternehmensindividuellen Gegebenheiten seinen allgemeinen Organisations- und Sorgfaltspflichten nachkommt.⁴

Die durch den Aufsichtsrat bzw. den Prüfungsausschuss zu überwachenden Corporate-Governance-Systeme IKS, RMS, IRS und Compliance-Management-Systeme (CMS) sind dabei weder im Gesetz noch in der Literatur eindeutig definiert. Zur Systematik des Zusammenspiels dieser Corporate-Governance-Systeme lehnt sich der IDW

1 Institut der Wirtschaftsprüfer in Deutschland: Entwurf eines IDW Prüfungsstandards: Grundsätze ordnungsmäßiger Prüfung von Risikomanagementsystemen (IDW EPS 981), abrufbar unter www.idw.de/idw/download/IDW_EPS_981.pdf?id=658492&property=Inhalt (Abruf: 8.6.2016), Tz. 1.

2 Entwurf eines Prüfungsstandards: Grundsätze ordnungsmäßiger Prüfung von Risikomanagementsystemen (IDW EPS 981), Tz. 2.

3 DCGK Ziff. 5.3.2.

4 IDW EPS 981 (Fn. 1), Tz. 4.

Prüfungsstandard an das COSO-Rahmenwerk zum unternehmensweiten Risikomanagement⁵ an.

„Auch wenn die Überwachungsfunktion höchstpersönlich von den Aufsichtsratsmitgliedern bzw. Prüfungsausschussmitgliedern wahrzunehmen ist und nicht an Dritte delegiert werden kann, kann es für den Aufsichtsrat von Interesse sein, einen Wirtschaftsprüfer mit der Prüfung einzelner oder mehrerer Corporate-Governance-Systeme als Grundlage für die eigene Beurteilung zu beauftragen. Auch der Vorstand kann ein Interesse daran haben, einen Wirtschaftsprüfer mit der Prüfung eines oder mehrerer dieser Systeme zu beauftragen. Die Prüfung der Wirksamkeit dieser Systeme durch einen unabhängigen Wirtschaftsprüfer kann dem objektivierten Nachweis der ermessensfehlerfreien Ausübung der Organisations- und Sorgfaltspflichten des Vorstands und des Aufsichtsrats dienen.“⁶

Gemäß Tz. 8 des Standards liegt die Zielsetzung einer nach IDW EPS 981 durchgeführten Systemprüfung in der Beurteilung, inwieweit das Unternehmen durch die Einrichtung eines RMS Vorsorge getroffen hat, wesentliche Risiken, die dem Erreichen der festgelegten Ziele des RMS entgegenstehen, rechtzeitig zu identifizieren, zu bewerten, zu steuern und zu überwachen. Ziel ist es dagegen nicht, eine Aussage darüber zu treffen, ob sämtliche Risiken von dem zu prüfenden RMS identifiziert und adressiert wurden und ob einzelne von den gesetzlichen Vertretern oder den nachgeordneten Entscheidungsträgern eingeleitete und durchgeführte Maßnahmen als Reaktion auf erkannte und beurteilte Risiken geeignet und wirtschaftlich sinnvoll sind. Die Prüfung ist auch nicht darauf ausgerichtet, ein Prüfungsurteil über den Fortbestand des Unternehmens zu erteilen.⁷

„Dabei ist die Prüfung des RMS nach IDW EPS 981 auch von der Prüfung des gem. § 91 Abs. 2 AktG einzurichtenden Überwachungssystems zur frühzeitigen Erkennung von den Fortbestand der Gesellschaft gefährdenden Entwicklungen (sog. „Risikofrüherkennungssystem“) nach § 317 Abs. 4 HGB zu unterscheiden. Die Prüfung des Risikofrüherkennungssystems umfasst zwar die Grundelemente Risikoidentifikation, Risikobeurteilung, Risikokommunikation und Überwachung, nicht aber die *Risikosteuerung*. Die Reaktionen des Vorstands auf erfasste und kommunizierte Risiken selbst sind somit nicht Gegenstand der Maßnahmen i. S. d. § 91 Abs. 2 AktG und damit auch nicht Gegenstand der Prüfung nach § 317 Abs. 4 HGB. Ferner ist anders als der Prüfungsgegenstand i. S. d. IDW EPS 981 die Prüfung des Risikofrüherkennungssystems nach § 317 Abs. 4 HGB nur auf bestandsgefährdende Risiken ausgerichtet. Bei der Prüfung nach § 317 Abs. 4 HGB werden jedoch alle Zielkategorien des unternehmensweiten Risikomanagements betrachtet und nicht nur strategische und operative Risiken.“⁸

Das Risikomanagementsystem ist die Ausgangslage jeglicher Überwachung. Die gesetzlichen Vertreter müssen sich von den wesentlichen Geschäftsrisiken Kenntnis verschaffen. Die Umsetzung der beschlossenen Maßnahmen zur Risikominimierung müssen in einem angemessenen Unternehmens- und Kontrollumfeld mittels des IKS und bezogen auf Compliance mittels des CMS sichergestellt und nachvollziehbar dokumentiert werden.⁹

II. Anforderungen an ein RMS gemäß EPS 981

Ein wirksames RMS ist integraler Bestandteil der Corporate Governance des Unternehmens und erfüllt die Anforderungen an Vorstand, Aufsichtsrat und Prüfungsausschuss nach §§ 130, 30, 9 OWiG sowie § 93 Abs. 1 AktG, § 107 Abs. 3 AktG. Mit der Einrichtung eines RMS tragen die Verantwortlichen Sorge, wesentliche Risiken, die dem

Erreichen der festgelegten Ziele des RMS entgegenstehen, rechtzeitig zu identifizieren, zu bewerten, zu steuern und zu überwachen.

Wesentliche Risiken sind dabei zum einen aus dem strategischen Umfeld abzuleiten, also solche, die dem Erreichen der strategischen Unternehmensziele entgegenstehen. Hierbei ist eine konzernweite Risikobetrachtung maßgeblich. Eine Eingrenzung auf einzelne Tochtergesellschaften, Unternehmensprozesse oder ausgewählte Abteilungen eines Unternehmens, ist daher nicht möglich bzw. sinnvoll abbildbar.¹⁰

Zum anderen umfassen die wesentlichen Risiken die operativen (betrieblichen) Risiken und somit die Risiken, die aus der Geschäftstätigkeit bzw. den Leistungserstellungsprozessen abgeleitet werden und dem Erreichen der aus den strategischen Zielen abgeleiteten operativen Zielen entgegenstehen.¹¹

III. Bestandteile des EPS 981

Die Struktur des EPS 981 erfolgt analog zum IDW PS 980 mit der differenzierteren Betrachtung der Risikoidentifikation und Risikobewertung und der Bezeichnung der Risikosteuerung, was in der Logik des PS 980 dem Compliance-Programm als die Ableitung von Compliance-Risiko minimierenden Maßnahmen entspricht.

Der EPS 981 lehnt sich in der Darstellung der *acht Elemente* in seiner Systematik an das COSO-Rahmenwerk zum unternehmensweiten Risikomanagement an, welches in der untenstehenden Abbildung dargestellt wird. Dabei wird die Notwendigkeit betont, bei der Konzeption des Risikomanagementsystems – und somit auch entsprechend bei der Prüfung – die Grundelemente in ihrer zueinander stehenden Wechselwirkung zu beachten, die in die entsprechenden Geschäftsabläufe eingebunden sind.

Die Grundelemente werden im Prüfungsstandard, wie nachfolgend skizziert, beschrieben. Die *Risikokultur*¹² als Teil der Unternehmenskultur umfasst die grundsätzliche Einstellung und die Verhaltensweisen beim Umgang mit Risikosituationen. Sie beeinflusst maßgeblich das Risikobewusstsein im Unternehmen und bildet die Grundlage für ein wirksames RMS.

Die *Ziele des RMS*¹³ sind darauf ausgerichtet sicherzustellen, dass die Unternehmensziele entsprechend der Risikostrategie erreicht werden. Die unternehmenspolitischen Zielsetzungen und insbesondere die Unternehmensstrategie bilden die Ausgangsbasis für die Ableitung einer Risikostrategie und ein systematisches Risikomanagement des Unternehmens. In der Risikostrategie wird festgelegt, in welchem Ausmaß unter Berücksichtigung der Risikotragfähigkeit des Unternehmens Risiken eingegangen werden sollen („Risikoappetit“), ergänzt durch unternehmerische Vorgaben zum erwünschten Umgang mit Risiken in Form einer Risikopolitik.

5 Unternehmensweites Risikomanagement – Übergreifendes Rahmenwerk (COSO ERM), abrufbar unter www.coso.org/-ERM.htm (Abruf: 8.6.2016).

6 IDW EPS 981 (Fn. 1), Tz. 6.

7 IDW EPS 981 (Fn. 1), Tz. 8.

8 IDW EPS 981 (Fn. 1), Tz. 13.

9 Risikomanagementsystem, Internes Kontrollsystem & Compliancemanagementsystem – Grundlagen und Ausgestaltungsformen, *Gnädiger*, StuB 2013, 187.

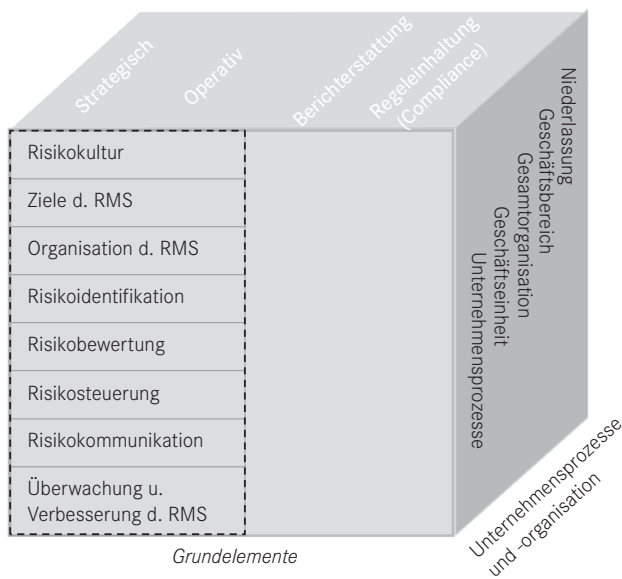
10 IDW EPS 981 (Fn. 1), Tz. 9.

11 IDW EPS 981 (Fn. 1), Tz. 10.

12 IDW EPS 981 (Fn. 1), Tz. A18.

13 IDW EPS 981 (Fn. 1), Tz. A19.

Abbildung: Abgrenzung der Teilbereiche¹⁴



Von entscheidender Bedeutung für das RMS sind eine transparente und eindeutige *Aufbauorganisation*¹⁵ sowie eine klar definierte *Ablauforganisation*. Verantwortungsbereiche und Rollen sind klar geregelt, abgegrenzt, kommuniziert und dokumentiert. Die Aufgabenträger erfüllen die erforderlichen persönlichen und fachlichen Voraussetzungen. Es stehen ausreichende Ressourcen für Risikomanagement-Maßnahmen zur Verfügung (insb. Personen, Technologie, Hilfsmittel). Die wesentlichen Regelungen zur Aufbau- und Ablauforganisation des Risikomanagements sind dokumentiert und verbindlich vorgegeben.

Die *Risikoidentifikation*¹⁶ umfasst die regelmäßige, systematische Analyse von internen und externen Entwicklungen und Ereignissen, die zu negativen oder positiven Abweichungen von den festgelegten Zielen des RMS führen können. Risiken werden systematisch beurteilt,¹⁷ typischerweise im Hinblick auf Eintrittswahrscheinlichkeit und möglicher Auswirkungen. Bewertungsverfahren und -kriterien sind (auch für nicht quantifizierbare Risiken) eindeutig definiert. Dies umfasst die Verwendung einer Bewertungssystematik, die es erlaubt, die Bedeutung und den Wirkungsgrad von Risikosteuerungsmaßnahmen einzuschätzen. Zu Risikobewertungen findet man in der Unternehmenspraxis deutlich unterschiedliche Herangehensweisen von einer einfachen Klassifizierung („gering, mittel, hoch“) bis hin zur systematischen Aggregation von Risiken und Analyse von Risikointerdependenzen.

Auf der Grundlage der identifizierten und bewerteten Risiken trifft die Unternehmensleitung Entscheidungen über Maßnahmen zur *Risikosteuerung*¹⁸ (Risikovermeidung, Risikoreduktion, Risikoteilung bzw. -transfer sowie Risikoakzeptanz). Als Bezugsrahmen dienen die festgelegten Ziele des RMS.

Die *Risikokommunikation*¹⁹ gewährleistet einen angemessenen Informationsfluss im RMS. Dies umfasst einen standardisierten Prozess auf der Basis konkreter Zuständigkeiten, Periodizitäten, Schwellenwerte und Berichtsformate. Für eilbedürftige Risikomeldungen ist ein separater Berichtsprozess etabliert, der eine zeitnahe Übermittlung der relevanten Informationen sicherstellt. Für die Risikobeurteilung werden die entscheidungsrelevanten Informationen gesammelt, auf ihre Zuverlässigkeit überprüft und aktualisiert. Die Angemessenheit

und Wirksamkeit des RMS werden durch prozessintegrierte und prozessunabhängige Kontrollen überwacht.

Voraussetzung für die Überwachung ist eine angemessene Dokumentation des RMS. Die Ergebnisse der Überwachungsmaßnahmen (insb. festgestellte Mängel im RMS) werden in geeigneter Form berichtet und ausgewertet, damit die erforderlichen Maßnahmen zur *Verbesserung* des Systems und zur Beseitigung von Mängeln ergriffen werden können.²⁰

Aus der Grafik oben geht auch die Abgrenzung bzw. die notwendige Interaktion zwischen den Corporate Governance-Elementen hervor, insbesondere in Hinblick auf ein wirksames CMS. Diese Systematik in einer übergeordneten Managementstruktur und ihre Bedeutung für die Pflichterfüllung des Aufsichtsrates spiegelt sich analog in den Möglichkeiten des Prüfungsvorgehens wider.

IV. Prüfung nach EPS 981 im Vergleich zum PS 980

Auch in den Möglichkeiten einer Prüfung und einem entsprechenden Prüfungsurteil und des damit einhergehenden Grades an Sicherheit gleicht der IDW EPS 981 dem IDW PS 980. Prüfungsgegenstand ist eine *Beschreibung des RMS*, in dem die Aussagen des Unternehmens über das bestehende System zur Risikoidentifizierung, -bewertung und -steuerung enthalten sind. Ziel ist schließlich der Nachweis eines wirksamen RMS. Bei einer entsprechenden Prüfung urteilt der Prüfer, ob die in einem bestimmten definierten und zur Prüfung beauftragten Zeitraum implementierten²¹ Regelungen des RMS in der RMS-Beschreibung in Übereinstimmung mit den angewandten RMS-Grundsätzen in allen wesentlichen Belangen angemessen dargestellt²² sind – und ob diese während des geprüften Zeitraums geeignet und wirksam waren, mit hinreichender Sicherheit die wesentlichen Risiken, die dem Erreichen der festgelegten Ziele des RMS entgegenstehen, rechtzeitig zu erkennen, zu bewerten, zu steuern und zu überwachen.²³

Tabelle: IDW EPS 981 im Vergleich zum IDW PS 980

IDW Prüfungsstandard	EPS 981	PS 980
Konzeptionsprüfung		✓
Angemessenheitsprüfung (zeitpunktbezogen)	✓	✓
Wirksamkeitsprüfung (zeitraumbezogen)	✓	✓
Skalierbarkeit der Prüfung	✓	✓
Projektbegleitende Prüfung	✓	✓

14 IDW EPS 981 (Fn. 1), Tz. A3.
 15 IDW EPS 981 (Fn. 1), Tz. A20.
 16 IDW EPS 981 (Fn. 1), Tz. A21.
 17 IDW EPS 981 (Fn. 1), Tz. A22.
 18 IDW EPS 981 (Fn. 1), Tz. A23.
 19 IDW EPS 981 (Fn. 1), Tz. A24.
 20 IDW EPS 981 (Fn. 1), Tz. A25.
 21 IDW EPS 981 (Fn. 1), Tz. 27.
 22 IDW EPS 981 (Fn. 1), Tz. 25.
 23 IDW EPS 981 (Fn. 1), Tz. 28.

Darüber hinaus räumt der Prüfungsstandard die Möglichkeit ein, nur einzelne Teilbereiche zur Prüfung und Bestätigung zu beauftragen. Die Skalierbarkeit der Prüfung ist auch hier möglich. Der Prüfungsstandard unterscheidet dabei explizit zwischen den strategischen Risiken, deren Prüfung separat beauftragt werden kann, die jedoch entsprechend ihrer Ausrichtung konzernweit betrachtet werden müssen. Bei der Prüfung von operativen Risikoarten schlägt der Prüfungsstandard eine mögliche Abgrenzung von Teilbereichen nach Unternehmensfunktionen oder -prozessen vor, die separat beauftragt werden können: etwa nach Risiken aus Unternehmensfunktionen (funktionale Sicht) wie Risiken in der Beschaffung, in der Produktion, beim Absatz, Risiken aus Unterstützungsfunktionen, wie bspw. dem Finanz- oder dem Personalwesen oder eben nach Risiken aus diversen Prozessen (prozessuale Sicht). Dies umfasst sowohl Kernprozesse, wie den Beschaffungs- oder Vertriebsprozess, unterstützende Prozesse, wie etwa der Qualitätssicherung, als auch Management-Prozesse, die sich bspw. mit der Ressourcen- und Budgetplanung, der Personalplanung und -entwicklung oder dem Management von Großprojekten befassen. Schließlich besteht analog zum PS 980 die Möglichkeit, einzelne Organisationseinheiten (Geschäftsbereiche, Funktionen, Tochtergesellschaften oder Regionen) abgegrenzt prüfen zu lassen. Dabei sind jeweils die strategischen Risiken zu betrachten.

In der Darstellung der operativen Risiken wird deutlich, dass es Schnittstellen zwischen originären Compliance- und Risikomanagement-Prozessen gibt – sowohl in der Ausgestaltung als auch dann in der Prüfung dieser Prozesse und ihrer inhärenten Risiken. Exemplarisch wird dies an dem Beschaffungsprozess deutlich. Während aus der Compliance-Sicht der Fokus auf Aspekte wie die Sicherstellung eines Vendor Integrity Screenings oder die Integration bestimmter Compliance-Klauseln in den Verträgen gelegt wird, liegt aus operativer Risikosicht der Fokus auf Risiken wie der Ausfall eines Dienstleisters, gar eines wichtigen Zulieferers, was u. U. durch Non-Compliance verursacht wird. An diesem Beispiel wird die Komplexität einer gelingenden Governance ebenso deutlich wie die enge Verzahnung der einzelnen Bereiche und die daraus hervorgehende Notwendigkeit, jedes Governance-Element in Wirksamkeit des jeweils eigenen Managementsystems zu betrachten als auch die Wechselwirkung, die relevanten Schnittstellen und schließlich das Zusammenspiel hin zu einem ganzheitlichen, wirksamen Corporate Governance-Management.

Ein Risikomanagementsystem sollte niemals isoliert implementiert werden, sondern immer als integraler Bestandteil eines übergeordneten Managementsystems eines Unternehmens betrachtet und konzipiert werden. Ein solches System umfasst die Unternehmensprozesse einer Good Governance ebenso wie Strategie- und Planungsprozesse, die der Entscheidungsfindung bei operativen Tätigkeiten, bei der Überwachung und bei der Berichterstattung zu Grunde liegen, um entsprechend Verantwortlichkeiten klar zuzuordnen und nachzuvollziehen.²⁴

Mit der Prüfung des RMS nach IDW EPS 981 erhalten Unternehmen einen unabhängigen und objektivierten Nachweis darüber, dass ihr RMS angemessen und wirksam ist. Einen hinreichenden Nachweis, dass Vorstand und Aufsichtsrat ihren Aufsichtspflichten i. S. v. §§ 130, 30, 9 OWiG, § 93 Abs. 1 und § 107 Abs. 3 AktG nachgekommen sind, soweit sie das RMS betreffen, kann nur die Wirksamkeitsprüfung erbringen. Neben der risikobegrenzenden Wirkung kann eine RMS-Prüfung als „Stresstest“ für das Unternehmen verstanden werden, der dazu beiträgt, ggf. bestehende Schwächen (z. B. Regelungslücken in Systemen) zu erkennen und das System zu verbessern.²⁵

V. Fazit

Mit dem EPS 981 wird für Vorstand, Aufsichtsrat und Prüfungsausschuss, die eine Wirksamkeit der Corporate-Governance-Elemente sicherstellen müssen, eine weitere Grundlage geschaffen, die Systematik von Risikomanagementsystemen, in Anlehnung an das COSO-Rahmenwerk, zu gestalten, zu überwachen und ggf. auch extern prüfen und bestätigen zu lassen.

Entscheidend werden das effektive Management und das daraus resultierende Reporting im Zusammenspiel der verschiedenen Corporate-Governance-Elemente sein. Neben dem seit 2011 existierenden Prüfungsstandard zur Prüfung von Compliance-Management-Systemen (PS 980) und dem neuen EPS 981 ist zu erwarten, dass Standards für die Prüfung des internen Kontrollsystems sowie der Internen Revision auf den Markt kommen werden. Vor dem Hintergrund ineinandergreifender Systematiken wird so der Rahmen für eine ganzheitliche, managementsystembezogene Erfüllung der Überwachungspflichten geschaffen.

AUTOREN



Markus Link ist Partner im Bereich Capital Markets bei Deloitte und leitet den Bereich Corporate Governance Assurance. Er verfügt über langjährige Erfahrung als Wirtschaftsprüfer internationaler Konzerne und betreut kapitalmarktorientierte Unternehmen im Rahmen gesetzlicher Abschlussprüfungen sowie bei der Prüfung von Corporate-Governance-Systemen.



Dr. Antonia Steßl promovierte als Soziologin über effektives Compliance-Management und ist Expertin für Corporate Governance Assurance bei Deloitte. Ihr Fokus liegt in der Beratung und Prüfung von Corporate-Governance-Systemen. Zielsetzung ist dabei die Erarbeitung haftungsreduzierender Maßnahmen unter Sicherstellung der Akzeptanz bei allen Beteiligten.

24 Abrufbar unter www.ifac.org/publications-resources/bolt-built (Abruf: 8.6.2016).

25 Schmidt, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, 3. Aufl. 2016, § 45 Wirtschaftsprüfung und CMS Prüfung, Rn. 14.