Erfahrung nutzen, Zukunft sichern.

DIIR Deutsches Institut für Interne Revision e.V.

Theodor-Heuss-Allee 108
60486 Frankfurt am Main
Telefon (069) 713769-0
Fax (069) 713769-69
www.diir.de
info@diir.de

Geschäftsführung:
Dorothea Mertmann
USt-ID DE 114235123
Vereinsregisternummer:
Amtsgericht Frankfurt
am Main VR 5326

DIIR – Deutsches Institut für Interne Revision e.V. Theodor-Heuss-Allee 108 60486 Frankfurt am Main

An die
Geschäftsstelle des
Instituts der Wirtschaftsprüfer in Deutschland e.V.
Tersteegenstraße 14
40474 Düsseldorf

Per Email an: stellungnahmen@idw.de

Frankfurt am Main
28. September 2016

Stellungnahme zum Entwurf eines Prüfungsstandards: Grundsätze ordnungsmäßiger Prüfung von Risikomanagementsystemen (IDW EPS 981)

Sehr geehrte Damen und Herren,

wir bedanken uns für die Möglichkeit, Änderungs- und Ergänzungsvorschläge zu dem von Ihnen veröffentlichten Entwurf eines Prüfungsstandards: Grundsätze ordnungsmäßiger Prüfung von Risikomanagementsystemen (IDW EPS 981) einzureichen.

Wir möchten Ihnen im Folgenden zunächst einen kurzen Überblick über das DIIR und die Rolle und Aufgaben der Internen Revision geben, um anschließend auch auf den Hintergrund zur Abgabe einer Stellungnahme und der beabsichtigen Zielsetzung einzugehen. Im Anschluss finden Sie unsere detaillierten Änderungs- und Ergänzungsvorschläge zu einzelnen Abschnitten des IDW EPS 981.

Das DIIR – Deutsches Institut für Interne Revision e.V.

Das DIIR – Deutsches Institut für Interne Revision e.V. wurde 1958 als gemeinnützige Organisation gegründet und zählt heute mehr als 2.900 Firmenmitglieder und persönliche Mitglieder aus allen Bereichen der Wirtschaft, Verwaltung und Wissenschaft, darunter aus allen DAX 30-Unternehmen und dem Großteil aller HDAX-Unternehmen. Das DIIR nimmt die fachliche Interessenvertretung der Internen Revision in Deutschland wahr und unterstützt die in der Internen Revision tätigen Fach- bzw. Führungskräfte u.a. mit der Bereitstellung von Revisionsstandards.

Rolle und Aufgaben der Internen Revision

Die Einrichtung einer Internen Revision in einem Unternehmen ergibt sich u.a. aus aktienrechtlichen Vorschriften (z.B. § 91 Abs. 2 AktG, § 93 Abs. 1 Satz 1 AktG, § 107 Abs. 3 Satz 2 AktG) mit Ausstrahlungswirkung auf andere Rechtsformen sowie aus spezialgesetzlichen Regelungen (z.B. § 25a KwG, § 30 VAG).

Die Definition der Internen Revision ist in den allgemein anerkannten Internationalen Grundlagen für die berufliche Praxis der Internen Revision des IIA wie folgt festgelegt:

„Die Interne Revision erbringt unabhängige und objektive Prüfungs- und Beratungsdienstleistungen, welche darauf ausgerichtet sind, Mehrwerte zu schaffen und die Geschäftsprozesse zu verbessern. Sie unterstützt die Organisation bei der Erreichung ihrer Ziele, indem sie mit einem systematischen und zielgerichteten Ansatz die Effektivität des Risikomanagements, der Kontrollen und der Führungs- und Überwachungsprozesse bewertet und diese verbessern hilft."

Eine der Kernaufgaben der Internen Revision ist es also, das Risikomanagementsystem in einem Unternehmen zu beurteilen und zu dessen Verbesserung beizutragen. Die Anforderungen an die Prüfung des Risikomanagements ergeben sich für die Interne Revision vor allem aus den Internationalen Grundlagen für die berufliche Praxis der Internen Revision (IPPF) des Institute of Internal Auditors (IIA), dem globalen Berufsverband der Internen Revision, und dem DIIR Revisionsstandard Nr. 2 „Prüfung des Risikomanagements durch die Interne Revision".

Zielsetzung der Stellungnahme des DIIR zum IDW EPS 981

DIIR und IDW haben bereits bei der Erarbeitung eines gemeinsamen Standards zur Prüfung des Internen Revisionssystems (veröffentlicht als DIIR Revisionsstandard Nr. 3 bzw. IDW EPS 983) vertrauensvoll und gut zusammengearbeitet, um einen praxisbezogenen Standard mit einheitlichen Anforderungen an die Einrichtung und die Beurteilung eines Internen Revisionssystems herauszugeben.

Aus unserer Sicht ist es für eine effektive Corporate Governance unbedingt erforderlich, dass die Anforderungen, die an die Beurteilung der Angemessenheit und Wirksamkeit von Corporate Governance Systemen gestellt werden, in den beruflichen Standards der Internen Revision und der Wirtschaftsprüfer miteinander in Einklang stehen. Dies ist eine grundlegende Voraussetzung dafür, dass die entsprechenden Verfahren und Maßnahmen wirksam und wirtschaftlich in einem Unternehmen eingerichtet werden können, und dafür, dass sich die mit der Überwachung der eingerichteten Systeme befassten Internen Revisoren und, bei entsprechender Beauftragung, Wirtschaftsprüfer reibungslos und möglichst effizient abstimmen und zusammenarbeiten können.

Daher möchten wir die Gelegenheit nutzen, um unseren Input hinsichtlich der Prüfung von Risikomanagementsystemen in den IDW Prüfungsstandard einfließen zu lassen mit dem Ziel, auch hier möglichst einheitliche Anforderungen für den Berufsstand der Wirtschaftsprüfer und der Internen Revision sicherzustellen.

Anmerkungen zum IDW EPS 981

Nachfolgend haben wir unsere Anmerkungen zum IDW EPS 981 bezogen auf einzelne Abschnitte und Textziffern des Entwurfs zusammengefasst:

1 Vorbemerkungen, Textziffer 1ff.:

In den Vorbemerkungen des IDW EPS 981 werden die Überwachungsaufgaben des Prüfungsausschusses bzw. Aufsichtsrats nach § 107 Abs. 3 Satz 2 AktG hinsichtlich des Internen Kontrollsystems, des Risikomanagementsystems und des Internen Revisionssystems dargestellt. Zur Systematik des Zusammenspiels der

verschiedenen Corporate Governance Systeme verweist der Entwurf auf das COSO-Rahmenwerk.

Nach Tz. 1 ist es das Ziel des IDW EPS 981, den Inhalt einer Prüfung des Risikomanagementsystems zu verdeutlichen. Dazu gehört unseres Erachtens auch die Abgrenzung der einzelnen Corporate Governance Systeme, die der Überwachung des Prüfungsausschusses bzw. Aufsichtsrats unterliegen und als Prüfungsgegenstand der einzelnen vom IDW entwickelten GRC-Prüfungsstandards vorgesehen sind (IDW PS 980-983).

Wir weisen darauf hin, dass zur Beschreibung der Abgrenzung der Corporate Governance Systeme im Sinne der 8. EU-Richtlinie von der European Confederation of Institutes of Internal Auditing (ECIIA) und der Federation of European Risk Management Associations (FERMA) das "Three-Lines-of Defense Modell" entwickelt und veröffentlicht worden ist. [1] Das Three-Lines-of Defense Modell hat sich innerhalb weniger Jahre etabliert und spiegelt sich in der Organisation eines überwiegenden Teils deutscher Unternehmen wider.[2]

Neben seiner hohen Bekanntheit und weiten Verbreitung ist das Modell unseres Erachtens sehr gut geeignet, um auch Aufsichtsräten und Vorständen die Struktur einer guten Corporate Governance und die Abgrenzung einzelner Funktionen innerhalb der Corporate Governance nahe zu bringen. Auch IDW EPS 983 greift auf das Three-Lines-of-Defense Modell zurück, um die Funktion eines Internen Revisionssystems innerhalb der Corporate Governance zu beschreiben (IDW EPS 983, Tz. 10).

Wir empfehlen daher, in den Vorbemerkungen des Standards die Funktion eines Risikomanagementsystems, sowie dessen Abgrenzung zum Internen Kontrollsystem und Internen Revisionssystems, anhand des Three-Lines-of-Defense Modells kurz zu beschreiben.

1 Vorbemerkungen, Textziffer 6:

In Tz. 6 wird dargestellt, dass sowohl der Aufsichtsrat als auch der Vorstand ein Interesse daran haben können, die Wirksamkeit der eingerichteten Corporate Governance Systeme durch einen Wirtschaftsprüfer beurteilen zu lassen.

Wir regen an, in den Anwendungshinweisen auch einen Hinweis aufzunehmen, dass bei der Beurteilung der eingerichteten Systeme eine Abstimmung und Zusammenarbeit zwischen Wirtschaftsprüfer und Interner Revision erfolgen sollte, um einen effizienten Beurteilungsprozess, optimale Ergebnisse und damit auch einen größtmöglichen Mehrwert für das Unternehmen zu generieren.

[1] Vgl. ECIIA/FERMA (2011), Guidance on the 8th EU Company Law Directive; IIA (2013), Position Paper: The Three Lines of Defense in Effective Risk Management and Control.
[2] Vgl. DIIR (2014), Enquête 2014 – Die Interne Revision in Deutschland, Österreich und der Schweiz, S.48 (erhältlich unter www.diir.de); Pohl/Eulerich (2014), Die Interne Revision in Deutschland, Österreich und der Schweiz, Zeitschrift Interne Revision (ZIR), 4/2014, S. 166.

Dazu schlagen wir folgende Formulierung einer neuen Tz. A3 vor:

Tz.	Formulierungsvorschlag
A3	Bei der Überwachung der eingerichteten Corporate Governance Systeme wird der Vorstand regelmäßig von der Internen Revision unterstützt. Dabei prüft die Interne Revision auch das unternehmensweite Risikomanagementsystem und andere Systeme der Corporate Governance. Bei der Beauftragung eines Wirtschaftsprüfers zur Prüfung des Risikomanagementsystems bzw. abgegrenzter Teilbereiche des Risikomanagementsystems ist daher eine Abstimmung und Zusammenarbeit zwischen Wirtschaftsprüfer und Interner Revision eine Voraussetzung dafür, einen möglichst effizienten Beurteilungsprozess, optimale Ergebnisse und damit auch einen größtmöglichen Mehrwert für das Unternehmen zu generieren.

1 Vorbemerkungen, Textziffer 13:

In Tz. 13 werden als Grundelemente einer Prüfung des Risikofrüherkennungssystems nach § 317 Abs. 4 HGB Risikoidentifikation, Risikobeurteilung, Risikokommunikation und Überwachung genannt.

Hier sollte unseres Erachtens „Ziele des RMS“, „Organisation des RMS“ und „Risikokultur“ ergänzt werden, um Einklang mit IDW EPS 340 (Tz. 5, 9 und 13f.) sowie den Grundelementen des IDW EPS 981 (Tz. 30ff.) herzustellen.

Dazu schlagen wir folgende Formulierung vor:

Tz.	Formulierung aktueller IDW EPS 981	Formulierungsvorschlag
13	Die Prüfung des RMS ist von der Prüfung des gemäß § 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. (…)	Die Prüfung des RMS ist von der Prüfung des gemäß § 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 **Ziele des RMS, Risikokultur, Organisation des RMS,** 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. (…)

2 Definitionen, Textziffern 17a), 17e) und 17f)

Der Begriff „Risiken“ wird in Tz. 17a) definiert als „mögliche künftige Entwicklungen oder Ereignisse, die zu einer für das Unternehmen negativen (Risiko im engeren Sinne) oder positiven (Chance) Zielabweichung führen können.“

Die Begriffe „Risikomanagement“ und „Risikomanagementsystem“ beziehen sich beide auf Chancen und Risiken und werden definiert als „strukturierter Umgang mit Chancen und Risiken im Unternehmen“ (Tz. 17e)) bzw. als „Gesamtheit der Regelungen, die einen strukturierten Umgang mit Chancen und Risiken im Unternehmen sicherstellt“ (Tz. 17f)).

Wir weisen darauf hin, dass der Begriff „Risiko“ in seiner Definition bereits die Chancen mit umfasst. Die Definitionen von „Risikomanagement“ bzw. „Risikomanagementsystem“ nennen explizit „Chancen und Risiken“. Daraus ergibt sich eine Dopplung in Bezug auf potentielle positive Zielabweichungen (unmittelbar über den Begriff „Chancen“ und mittelbar über die Definition „Risiko“) und damit unseres Erachtens eine nicht sachgerechte Schwerpunktsetzung auf „positive Zielabweichungen (Chancen)“, die ggf. auch zu einer unangemessenen Fokussierung Im Rahmen des Risikomanagements auf Chancen führen könnte. Wir regen an, die Definitionen der Begriffe „Risikomanagement“ bzw. „Risikomanagementsystem“ entsprechend anzupassen und nur den Begriff „Risiko“ zu verwenden sowie den Begriff „Chancen“ zu streichen. Über die Definition „Risiko“ wären Chancen im Sinne von „positiven Zielabweichungen“ mit umfasst.

Dazu schlagen wir folgende Formulierung vor:

Tz.	Formulierung aktueller IDW EPS 981	Formulierungsvorschlag
17	e) Risikomanagement – strukturierter Umgang mit Chancen und Risiken im Unternehmen. f) Risikomanagementsystem – Gesamtheit der Regelungen, die einen strukturierten Umgang mit Chancen und Risiken im Unternehmen sicherstellt (vgl. Tz. 30, Tz. A8 f.).	e) Risikomanagement – strukturierter Umgang mit ~~**Chancen und**~~ Risiken **(im Sinne von positiver und negativer Zielabweichung)** im Unternehmen. f) Risikomanagementsystem – Gesamtheit der Regelungen, die einen strukturierten Umgang mit ~~**Chancen und**~~ Risiken **(im Sinne von positiver und negativer Zielabweichung)** im Unternehmen sicherstellt (vgl. Tz. 30, Tz. A8 f.).

Wir empfehlen darüber hinaus, die Definition von Risiken im Sinne von positiver und negativer Zielabweichung auch in den sonstigen Prüfungsstandards des IDW (z.B. IDW PS 340) zu verwenden.

2 Definitionen, Textziffer 17d)

Das Begriffspaar „wesentliches Risiko“ wird in Tz. 17d) definiert als „Risiko, das – mit einer nicht nur vertretbar geringen Eintrittswahrscheinlichkeit – zu einer für das Unternehmen wesentlichen negativen oder positiven Zielabweichung führen kann“.

Durch diese Formulierung wird der Begriff „wesentlich“ (in „wesentliches Risiko“) mit dem Begriff „wesentlich“ („wesentliche…Zielabweichung“) definiert. Die Definition ist daher in der jetzigen Formulierung nicht geeignet. Wir empfehlen daher, den Begriff „wesentlich“ im Zusammenhang mit dem Begriff „Risiko“ neu zu definieren. Als „wesentlich“ könnte ein Risiko bspw. dann betrachtet werden, wenn die mögliche (d.h. mit einer nicht nur vertretbar geringen Eintrittswahrscheinlichkeit) Zielabweichung dazu führt, dass die Unternehmensziele nicht entsprechend der Risikostrategie (vgl. auch Tz. 30 bzw. Tz. A20) erreicht werden.

IDW EPS 981 enthält zwar in Tz. 49 bzw. Tz. A37ff. Ausführungen zur „Wesentlichkeit“, diese beziehen sich jedoch auf „wesentliche Fehler in der RMS-Beschreibung“ bzw. „wesentliche Mängel des RMS“ und sind unseres Erachtens nicht ohne weiteres übertragbar auf „wesentliche Risiken“.

Eine entsprechende Definition von „wesentliches Risiko“ könnte vor dem Hintergrund wie folgt formuliert werden:

Tz.	Formulierung aktueller IDW EPS 981	Formulierungsvorschlag
17	d) Wesentliches Risiko – Risiko, das – mit einer nicht nur vertretbar geringen Eintrittswahrscheinlichkeit – zu einer für das Unternehmen wesentlichen negativen oder positiven Zielabweichung führen kann.	d) Wesentliches Risiko – Risiko, das – mit einer nicht nur vertretbar geringen Eintrittswahrscheinlichkeit – zu einer für das Unternehmen ~~**wesentlichen**~~ negativen oder positiven Zielabweichung führen kann**, durch die die Unternehmensziele nicht entsprechend der Risikostrategie erreicht werden.**

Definitionen, Textziffer 17n)

Ein „Mangel des RMS“ ist in Tz. 17n) definiert als „Beanstandung hinsichtlich Identifizierung, Bewertung, Steuerung und Überwachung der Risiken, die dem Erreichen der festgelegten Ziele des RMS entgegenstehen.“

Bei der Prüfung des Risikomanagementsystems nach IDW EPS 981 handelt es sich um eine Systemprüfung. Dementsprechend wird in dem Entwurf auch klargestellt, dass das Ziel der Prüfung u.a. nicht ist, eine Aussage darüber zu treffen, ob sämtliche Risiken von dem zu prüfenden RMS identifiziert und adressiert wurden (Tz. 8). Die Definition ist daher unseres Erachtens so anzupassen, dass sich die Beanstandungen auf die implementierten Regelungen des RMS beziehen.

Dazu schlagen wir folgende Formulierung vor:

Tz.	Formulierung aktueller IDW EPS 981	Formulierungsvorschlag
17	n) Mangel des RMS – Beanstandung hinsichtlich der Identifizierung, Bewertung, Steuerung und Überwachung der Risiken, die dem Erreichen der festgelegten Ziele des RMS entgegenstehen.	n) Mangel des RMS – Beanstandung hinsichtlich der **implementierten Regelungen des RMS zur** Identifizierung, Bewertung, Steuerung und Überwachung der Risiken, die dem Erreichen der festgelegten Ziele des RMS entgegenstehen.

4 Grundelemente eines RMS, Textziffern 30 und A26

IDW EPS 981 nennt als eines der Grundelemente eines RMS die „Überwachung und Verbesserung des RMS“ (Tz. 30). Die Anwendungshinweise enthalten dazu weitere Ausführungen (Tz. A26). Dort wird im Zusammenhang mit der prozessunabhängigen Überwachung beispielhaft auch die Interne Revision genannt.

Wir möchten darauf hinweisen, dass die Interne Revision in Übereinstimmung mit dem Three-Lines-of-Defense-Modell als dritte Verteidigungslinie die Funktion in einem Unternehmen ist, die unabhängig und objektiv das Risikomanagement überprüft und dabei auch Funktionen der ersten und zweiten Verteidigungslinie (z.B. Compliance, Risikomanagement) mit einbezieht. Dies gilt vor allem für Unternehmen, bei denen, wie in Vorbemerkungen des IDW EPS 981 dargestellt ist, aufgrund von aktienrechtlichen Vorgaben neben einem Risikomanagementsystem u.a. auch ein Internes Revisionssystem einzurichten ist (Tz. 2ff.).

Wir empfehlen daher, die Rolle der Internen Revision vor dem Hintergrund dieser Ausführungen stärker hervorzuheben. Zudem wäre es unseres Erachtens hilfreich, wenn hinsichtlich der beschriebenen Art und Umfang der Überwachung auf die allgemein anerkannten Internationalen Grundlagen für die berufliche Praxis der Internen Revision (IPPF) des Institute of Internal Auditors und den DIIR Revisionsstandard Nr. 2 „Prüfung des Risikomanagements durch die Interne Revision“ verwiesen würde.

Dazu schlagen wir folgende Formulierung von Tz. A26 vor:

Tz.	Formulierung aktueller IDW EPS 981	Formulierungsvorschlag
A26	(…) Das RMS ist Bestandteil regelmäßiger prozessunabhängiger Überwachung (z.B. durch die Interne Revision). Die Überwachung beinhaltet auch regelmäßige Beurteilungen des RMS, die sowohl auf die Angemessenheit als auch auf dessen Wirksamkeit gerichtet sind. Gegenstand einer prozessunabhängigen Überwachung	(…) Das RMS ist Bestandteil regelmäßiger prozessunabhängiger Überwachung ~~**(z.B. durch die Interne Revision)**~~. **Diese wird in der Regel von der Internen Revision durchgeführt.** Die Überwachung beinhaltet auch regelmäßige Beurteilungen des RMS, die sowohl auf die Angemessenheit als auch auf

	können u.a. folgende Aspekte sein: (…)	dessen Wirksamkeit gerichtet sind. **Art und Umfang der Beurteilung des RMS durch die Interne Revision ergeben sich aus den Internationalen Grundlagen für die berufliche Praxis der Internen Revision (IPPF) des Institute of Internal Auditors und dem DIIR Revisionsstandard Nr. 2 „Prüfung des Risikomanagements durch die Interne Revision“.** Gegenstand einer prozessunabhängigen Überwachung können u.a. folgende Aspekte sein: (…)

Die im IDW EPS 981 genannten Grundelemente umfassen auch „Risikokultur“ und „Risikokommunikation“. Die beiden genannten Elemente stehen in Einklang mit IDW PS 980 („Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen“), der die Begriffe „Compliance-Kultur“ und „Compliance-Kommunikation“ verwendet. IDW EPS 982 („Grundsätze ordnungsmäßiger Prüfung des internen Kontrollsystems der Unternehmensberichterstattung“) verwendet die Begriffe „Kontrollumfeld“ und „Information und Kommunikation“. Die im COSO ERM verwendeten Begriffe sind „Internes Umfeld“ (Internal Environment) und „Information und Kommunikation“ (Information and Communication).

Die im IDW EPS 981 verwendeten Begriffe „Risikokultur“ und „Risikokommunikation“ scheinen hinter den entsprechenden Begrifflichkeiten in IDW EPS 982 und COSO ERM zurück zu bleiben. Nach unserem Verständnis ist die „Kultur“ eines Unternehmens Teil des „Internen Umfelds“. Das „Interne Umfeld“ umfasst aber noch weitere Aspekte. „Kommunikation“ setzt voraus, dass Informationen zunächst gesammelt und aufbereitet werden, bevor sie kommuniziert werden können. Die Beschreibung der Begriffe in Tz. 30 bzw. den dazugehörigen Anwendungshinweisen legt nahe, dass die verwendeten Begriffe im Sinne der Begriffe „Internes Umfeld“ und „Information und Kommunikation“ von COSO ERM zu verstehen sind. Wir schlagen daher vor, die Bezeichnung der Grundelemente des RMS in Anlehnung an die entsprechenden Formulierungen des IDW EPS 982 wie folgt anzupassen:

Tz.	Formulierung aktueller IDW EPS 981	Formulierungsvorschlag
30	Risikokultur: Die Risikokultur 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.	**Umfeld des RMS (einschl.** Risikokultur**): Das Umfeld des RMS stellt den Rahmen dar, innerhalb dessen die Regelungen des RMS eingeführt und angewendet werden. Es ist geprägt durch die Grundeinstellungen, das Problembewusstsein und die Verhaltensweisen, die**

	Risikokommunikation: Die Risikokommunikation 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.	**Risikokultur sowie durch die Rolle des Aufsichtsorgans („tone at the top“) in Bezug auf das RMS.** Die Risikokultur 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. Risiko**information und -** kommunikation: Die Risiko**information und –** kommunikation gewährleistet einen angemessenen Informationsfluss im RMS. **Dazu zählt, dass die erforderlichen Informationen in geeigneter und zeitgerechter Form eingeholt, aufbereitet und an die zuständigen Stellen im Unternehmen weitergeleitet werden.** 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.

In Anlehnung an COSO ERM aus dem Jahr 2004 werden als Grundelemente eines RMS zudem „Risikoidentifikation“ und „Risikobewertung“ genannt. Neuere Standards zum Risikomanagement wie z.B. ISO 31000:2009 bzw. ONR 49000ff:2014 heben darüber hinaus auch die „Risikoanalyse“ als eigenständigen Schritt im Rahmen des Risikomanagementprozesses hervor. Ohne die Prüfung der Risikoanalyse läuft der Prüfer Gefahr, diverse Fehlentwicklungen im Risikomanagementprozess zu übersehen oder falsch einzuschätzen. Dementsprechend weist der Standard ONR 49001 in seinem Anhang zur Prüfung des Risikomanagements auch auf Folgendes hin:

„21 Die Risikoanalyse schafft das Verständnis der Risiken unter Einschluss ihrer Ursachen und Auswirkungen. Dabei werden die technischen, organisatorisch-wirtschaftlichen sowie die menschlichen Ursachen des Risikos berücksichtigt.[3]“

Auch das DIIR hat sich im DIIR Revisionsstandard Nr. 2 zur Prüfung des Risikomanagements durch die Interne Revision eindeutig positioniert und die Risikoanalyse als einen wesentlichen Bestandteil eines Risikomanagementsystems identifiziert. Der Standard führt dazu u.a. aus:

„41 Die im Risikoinventar erfassten Risiken sind im Rahmen der Risikoanalyse hinsichtlich der Ursache-Wirkung-Zusammenhänge zu untersuchen sowie im Hinblick auf ihr Schadenspotenzial und ihre Eintrittswahrscheinlichkeit einzuschätzen (…).

42 (…)

43 Aufgabe der Internen Revision im Rahmen der Prüfung der Risikoanalyse und –bewertung ist neben der Feststellung der vollständigen Durchführung der Analyse für alle identifizierten Risiken vor allem die Beurteilung der Angemessenheit der angewandten Methoden. Darüber hinaus sind qualitative oder quantitative Analysen und Berechnungen in Stichproben nachzuvollziehen, um die korrekte Anwendung der Methoden festzustellen.[4]“

Wir empfehlen daher, die Grundelemente eines RMS (Tz.30) und die Anwendungshinweise entsprechend zu ergänzen und die „Risikoanalyse“ explizit mit aufzunehmen:

Tz.	Formulierung aktueller IDW EPS 981	Formulierungsvorschlag
30	Risikobewertung: Risiken werden systematisch beurteilt, typischerweise im Hinblick auf Eintrittswahrscheinlichkeit und mögliche 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. Die einzelnen Risikobewertungen werden sysematisch aggregiert. Risikointerdependenzen werden analysiert und berücksichtigt.	**Risikoanalyse und -bewertung**: **Die identifizierten Risiken werden im Rahmen der Risikoanalyse hinsichtlich ihrer Ursache-Wirkung-Zusammenhänge untersucht sowie** ~~**Risiken werden systematisch beurteilt, typischerweise**~~ im Hinblick auf Eintrittswahrscheinlichkeit und mögliche Auswirkungen beurteilt. 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

[3] Vgl. ONR 49001:2014, A.4 Inhalt des Risikomanagement-Systemaudits
[4] Vgl. DIIR Revisionsstandard Nr. 2 „Prüfung des Risikomanagementsystems durch die Interne Revision“

		einzuschätzen. Die einzelnen Risikobewertungen werden sysematisch aggregiert. Risikointerdependenzen werden analysiert und berücksichtigt.

4 Grundelemente eines RMS, Textziffer 33

In Tz. 33 wird ausgeführt, dass es einer Beauftragung des Wirtschaftsprüfers als RMS-Prüfer nicht entgegensteht, wenn der Wirtschaftsprüfer mit der Jahresabschlussprüfung für das Unternehmen beauftragt ist.

Art. 5 Abs. 1 Satz 2 Buchst. h der EU-Verordnung zur Abschlussprüfung sieht vor, dass der Abschlussprüfer eines Unternehmens von öffentlichem Interesse (sog. Public Interest Entity – PIE) keine Leistungen im Zusammenhang mit der Internen Revision des Unternehmens erbringen darf. Das IDW hat nach Veröffentlichung des IDW EPS 981 in seinem Positionspapier „EU-Regulierung und Abschlussprüfung“ zu dieser Vorschrift Stellung genommen.[5] Dabei vertritt das IDW die Auffassung, dass die genannte Regelung der EU-Verordnung sämtliche Prüfungs- und Beratungstätigkeiten des Abschlussprüfers eines Unternehmens von öffentlichem Interesse im Sinne der Tätigkeiten einer Internen Revision untersagt (Abschn. 6.3.15, S. 44f.). Dabei bezieht sich das IDW auf eine Definition der Tätigkeiten einer Internen Revision nach IESBA Code of Ethics (Tz. 290.192) [6]:

„Nach IESBA Code of Ethics, Tz. 290.192 zählen zu den Tätigkeiten der Internen Revision

a. die Überwachung von internen Kontrollen – Überprüfung von Kontrollen, Überwachung ihrer Funktion und Empfehlung von Verbesserungen dazu,
b. Untersuchung von Finanz- und Betriebsinformationen – Überprüfung der Maßnahmen zur Erkennung, Bewertung und Klassifizierung von Finanz- und Betriebsinformationen und zur Berichterstattung darüber, sowie besonderer Untersuchungen einzelner Sachverhalte, einschließlich der Detailprüfung von Geschäftsvorfällen, Salden und Verfahren,
c. die Überprüfung der Sparsamkeit, Wirtschaftlichkeit und Wirksamkeit der Geschäftstätigkeit, einschließlich der nichtfinanziellen Tätigkeiten einer Einheit, und
d. Überprüfung der Einhaltung von Gesetzen, anderen Rechtsvorschriften und sonstigen externen Anforderungen sowie der Einhaltung von Regelungen und Anweisungen des Managements und sonstigen internen Anforderungen“

Obwohl in dieser Definition des IESBA Code of Ethics das „Risikomanagement“ bzw. das „Risikomanagementsystem“ nicht explizit als Gegenstand der Tätigkeiten der Internen Revision aufgezählt wird, so dürfte unseres Erachtens die Prüfung des Risikomanagementsystems zumindest mittelbar in der Definition enthalten sein.

[5] Vgl. IDW (2016), EU-Regulierung und Abschlussprüfung, IDW-Positionspapier zu Inhalten und Zweifelsfragen der EU-Verordnung und der Abschlussprüferrichtlinie (erstmalig überarbeitete Fassung mit Stand: 11.04.2016).
[6] Vgl. IDW (2016), S. 44f.

Darüber hinaus weisen wir darauf hin, dass die Definition der Internen Revision nach den allgemein anerkannten Internationalen Grundlagen für die berufliche Praxis der Internen Revision (IPPF) des Institute of Internal Auditors (IIA) die Prüfung des Risikomanagements explizit als eine der Kernaufgaben der Internen Revision benennt:

„Die Interne Revision erbringt unabhängige und objektive Prüfungs- und Beratungsdienstleistungen, welche darauf ausgerichtet sind, Mehrwerte zu schaffen und die Geschäftsprozesse zu verbessern. Sie unterstützt die Organisation bei der Erreichung ihrer Ziele, indem sie mit einem systematischen und zielgerichteten Ansatz die Effektivität des Risikomanagements, der Kontrollen und der Führungs- und Überwachungsprozesse bewertet und diese verbessern hilft."

Wir empfehlen vor diesem Hintergrund noch einmal zu überprüfen, ob die Aussage in Tz. 33 zur Vereinbarkeit der Prüfung des Risikomanagementsystems mit der Jahresabschlussprüfung auch im Hinblick auf Unternehmen von öffentlichem Interesse und die Regelungen der EU-Verordnung in dieser allgemeinen Form aufrecht erhalten werden kann.

6 Auftragsannahme, Textziffer 35

Nach Tz. 35 hat der Wirtschaftsprüfer die Eignung des in der RMS-Beschreibung dargestellten Systems als Prüfungsgegenstand zu beurteilen.

Der IDW EPS 981 sieht vor, dass die Prüfung des Risikomanagementsystems auf bestimmte Teilbereiche begrenzt werden kann, so z.B. auf strategische Risiken oder operative Risiken einzelner Unternehmensprozesse (Tz. 9ff.). Durch eine Begrenzung auf Teilbereiche des Risikomanagementsystems wird auch der gemäß Tz. 35 zu beurteilende Prüfungsgegenstand beeinflusst.

Unseres Erachtens ist bei der Beurteilung des Prüfungsgegenstandes durch den Wirtschaftsprüfer auch die Angemessenheit des Zuschnitts des zu beurteilenden Risikomanagementsystems zu beurteilen. Grundsätzlich sollte das gesamte unternehmensweite Risikomanagementsystem Gegenstand der Prüfung sein. Eine Begrenzung auf einzelne Teilbereiche sollte nur aufgrund sachgerechter Gründe erfolgen. So sollte bspw. vermieden werden, dass eine Begrenzung auf bestimmte Teilbereiche willkürlich erfolgt oder der Prüfungsgegenstand vom geprüften Unternehmen nur deshalb auf eine bestimmte Weise „zugeschnitten" wird, um die Aufdeckung von Mängeln in relevanten Bereichen des Risikomanagementsystems zu verhindern. Wir regen daher an, dass die Beurteilung der Angemessenheit der Abgrenzung des Prüfungsgegenstandes explizit in Tz. 35 des Standards mit aufgenommen wird.

Dazu schlagen wir folgende Formulierung vor:

Tz.	Formulierung aktueller IDW EPS 981	Formulierungsvorschlag
35	Im Zusammenhang mit der Entscheidung über die Annahme eines Auftrags zur Durchführung einer RMS-Prüfung hat sich der Wirtschaftsprüfer Informationen über die Ausgestaltung	Im Zusammenhang mit der Entscheidung über die Annahme eines Auftrags zur Durchführung einer RMS-Prüfung hat sich der Wirtschaftsprüfer Informationen über

	des RMS und der zugrunde liegenden RMS-Grundsätze zu verschaffen, um die grundsätzliche Eignung des in der RMS-Beschreibung dargestellten Systems als Prüfungsgegenstand zu beurteilen. Diese Beurteilung hat anhand der in Tz. 30 dargestellten Grundelemente eines RMS zu erfolgen (vgl. Tz. A27 ff.).	die Ausgestaltung des RMS und der zugrunde liegenden RMS-Grundsätze zu verschaffen, um die grundsätzliche Eignung des in der RMS-Beschreibung dargestellten Systems als Prüfungsgegenstand zu beurteilen. Diese Beurteilung hat anhand der in Tz. 30 dargestellten Grundelemente eines RMS zu erfolgen (vgl. Tz. A27 ff.). **Dabei sind auch die Gründe für eine eventuelle Begrenzung der Prüfung auf bestimmte Teilbereiche des unternehmensweiten RMS zu berücksichtigen und dahingehend zu beurteilen, ob die Gründe vor dem Hintergrund der Erwartungen der Adressaten der Berichterstattung über die RMS-Prüfung sachgerecht sind.**

6 Verwendung der Arbeit der Internen Revision, Textziffern 70f. und A63f.

Die Regelungen zur Verwendung der Arbeiten der Internen Revision verweisen auf die Internationalen Grundlagen für die berufliche Praxis der Internen Revision (IPPF) des Institute of Internal Auditors.

Wir weisen darauf hin, dass die Qualität der Arbeit der Internen Revision auch von der Einhaltung der vom DIIR herausgegebenen Revisionsstandards, die die IPPF ergänzen und deren Anwendung in Deutschland unterstützen, abhängt. Bei der Beurteilung der Tätigkeiten der Internen Revision ist außerdem von Bedeutung, ob bei der Internen Revision ein „Quality Assessment" im Sinne des IPPF nach DIIR Revisionsstandard Nr. 3 „Prüfung von Internen Revisionssystemen (Quality Assessments)" (oder nach dem bis 2016 gültigen „DIIR Leitfaden zur Durchführung eines Quality Assessments") durchgeführt wurde.[7] Zudem hängt die Möglichkeit einer Verwendung der Arbeiten der Internen Revision auch davon ab, ob diese bezogen auf das Risikomanagement nach dem DIIR Revisionsstandard Nr. 2 „Prüfung des Risikomanagements durch die Interne Revision" durchgeführt wurden. Wir empfehlen daher Tz. A64 entsprechend zu ergänzen.

Dazu schlagen wir folgende Formulierung vor:

Tz.	Formulierung aktueller IDW EPS 981	Formulierungsvorschlag
A64	Bei der Beurteilung der Arbeit der internen Revision ist auch von Bedeutung, inwieweit die	Bei der Beurteilung der Arbeit der internen Revision ist auch von Bedeutung, inwieweit die

[7] DIIR und IDW haben gemeinschaftlichen einen Standard zur Prüfung von Internen Revisionssystemen erarbeitet. Das DIIR hat diesen als DIIR Revisionsstandard Nr. 3 „Prüfung von Internen Revisionssystemen (Quality Assessments)", das IDW hat zeitgleich den inhaltlich weitestgehend gleichlautenden IDW EPS 983 herausgegeben.

	Anforderungen aus den Internationalen Grundlagen für die berufliche Praxis der Internen Revision (IPPF) des IIA (The Institute of Internal Auditors) berücksichtigt wurden.	Anforderungen aus den Internationalen Grundlagen für die berufliche Praxis der Internen Revision (IPPF) des IIA (The Institute of Internal Auditors) **sowie der DIIR Revisionsstandards, insbesondere DIIR Revisionsstandard Nr. 2 zur Prüfung des Risikomanagements durch die Interne Revision,** berücksichtigt wurden. **Bei der Beurteilung der Arbeiten der Internen Revision sollte auch berücksichtigt werden, ob und mit welchem Ergebnis bei der Internen Revision ein „Quality Assessment“ im Sinne des IPPF nach DIIR Revisionsstandard Nr. 3 „Prüfung von Internen Revisionssystemen (Quality Assessments)“ (oder nach dem bis 2016 gültigen „DIIR Leitfaden zur Durchführung eines Quality Assessments“) durchgeführt wurde.**

Zudem weisen wir darauf hin, dass es sich bei dem Begriff „Interne Revision“ um einen feststehenden Begriff handelt und daher „Intern“ mit einem Großbuchstaben beginnt. Dies entspricht u.a. auch der Schreibweise in den allgemein anerkannten Internationalen Grundlagen für die berufliche Praxis der Internen Revision des IIA sowie in den DIIR Revisionsstandards (beides abrufbar unter www.diir.de) und im IDW EPS 983.

Daher ist der Begriff „interne Revision“ im IDW EPS 981 (und den sonstigen Prüfungsstandards des IDW) durchgehend „Interne Revision“ zu schreiben.

Anlage 1: Allgemein anerkannte RMS-Rahmenkonzepte

Allgemein anerkannte Rahmenkonzepte des RMS werden in Tz. 17j) definiert als „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“. Anlage 1 enthält eine nicht abschließende Aufzählung entsprechender Rahmenkonzepte.

Aufgrund ihrer Bedeutung insbesondere für Kreditinstitute und Finanzdienstleister empfehlen wir, die „Mindestanforderungen an das Risikomanagement“ (MaRisk BA) in die Aufzählung der Anlage 1 ebenfalls aufzunehmen.

DIIR Deutsches Institut für Interne Revision e.V.

Anlage 2: Berichterstattung über RMS-Prüfungen

In den Beispielen für die Berichterstattung in Anlage 2 heißt es:

„(…) Die für … (Beschreibung des zu prüfenden RMS bzw. der abgegrenzten Teilbereiche) implementierten Regelungen sind angemessen, wenn …und wenn sie implementiert sind“

Hier kommt es sprachlich zu einer Doppelung bei dem Begriff „implementiert“. Wir schlagen daher eine Anpassung der Formulierung wie folgt vor:

Tz.	Formulierung aktueller IDW EPS 981	Formulierungsvorschlag
Anlage 2	(…) Die für ... [Beschreibung des zu prüfenden RMS bzw. der abgegrenzten Teilbereiche] implementierten Regelungen des RMS sind angemessen, wenn sie geeignet sind, mit hinreichender Sicherheit die wesentlichen Risiken, die dem Erreichen der festgelegten Ziele des RMS entgegenstehen, rechtzeitig zu identifizieren, zu bewerten, zu steuern und zu überwachen, und wenn sie implementiert sind. (…)	(…) Die **in der RMS-Beschreibung** für ... [Beschreibung des zu prüfenden RMS bzw. der abgegrenzten Teilbereiche] ~~**implementierten**~~ **dargestellten** Regelungen des RMS sind angemessen, wenn sie geeignet sind, mit hinreichender Sicherheit die wesentlichen Risiken, die dem Erreichen der festgelegten Ziele des RMS entgegenstehen, rechtzeitig zu identifizieren, zu bewerten, zu steuern und zu überwachen, und wenn sie implementiert sind. (…)

Für Rückfragen stehen Ihnen Dorothea Mertmann (unter 069/713769-30 oder d.mertmann@diir.de) oder Christoph Scharr (unter 069/713769-20 oder c.scharr@diir.de) gerne zur Verfügung. Gerne besprechen wir unsere Anmerkungen mit Ihnen auch in einem persönlichen Gespräch.

Mit freundlichen Grüßen

Dorothea Mertmann
Geschäftsführerin

Christoph Scharr
Leiter Grundsatzabteilung