Risk Management Association e. V.
Englmannstraße 2
D-81673 München
Tel.: +49.(0)1801.762.835
Fax: +49.(0)1801.762.329
E-Mail: office@rma-ev.org

RiskManagement
Association e.V.

Stellungnahme

zum

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

Sehr geehrte Damen und Herren,

vielen Dank für die Möglichkeit einer Stellungnahme zu dem von Ihnen veröffentlichten Entwurf eines neuen Standards zur Prüfung des Risikomanagementsystems (IDW EPS 981).

Zunächst erlauben Sie uns bitte, die Risk Management Association e.V. mit ihren Zielen und Aufgaben kurz vorzustellen und dann die Eckpunkte und Zielsetzung unserer Stellungnahme zu erläutern. Anschließend finden Sie ergänzende Erläuterungen und konkrete Verbesserungsvorschläge.

Die Risk Management Association e.V. (www.rma-ev.org)

Die Risk Management Association e.V. (RMA) ist die unabhängige Interessenvertretung für das Thema Risikomanagement im deutschsprachigen Raum mit Fokus auf Unternehmen der Realwirtschaft. Als Kompetenzpartner und Impulsgeber ist die RMA erster Ansprechpartner für Informationen, den unternehmensübergreifenden Dialog sowie die Weiterentwicklung des Risikomanagements. Zu den über 450 Mitgliedern der RMA zählen internationale Konzerne, mittelständische Unternehmen sowie Privatpersonen aus Wirtschaft, Wissenschaft und dem öffentlichen Sektor.

Mithilfe eigener Fachgremien befasst sich die RMA mit den wichtigsten Risikomanagementthemen wie beispielsweise Standards im Risikomanagement, Verzahnung von Risikomanagement und Controlling, Compliance Risk Management, IT-Risiken und Reputationsrisiken.

Die RMA bildet ein professionelles Netzwerk aus Experten und Vordenkern aus dem Risikomanagement-Umfeld. Damit fördert die RMA ein nachhaltiges Vorgehen und bringt sich maßgeblich in die Diskussion und Ergebnisfindung im Risikomanagement ein.

Strategische Kooperationen mit verwandten Verbänden und Interessengruppen, darunter die ISACA, der Internationale Controller Verein und insbesondere das Deutsche Institut für Interne Revision (DIIR), stärken diese Ziele.

Mit dem DIIR arbeiten wir derzeit in einem gemeinsamen Arbeitskreis an der Klärung von Fragen der Zusammenarbeit zwischen Interner Revision und Risikomanagement und an einem Leitfaden als Ergänzung zum DIIR Standard Nr.2 zur Prüfung des Risikomanagements.

Zielsetzung

Als Verband von Risikomanagern versteht sich die RMA als deren Interessenvertretung. Der Risikomanager hat sich als Beruf erst mit KontraG seit 1998 etabliert und entwickelte sich stetig vom Risikobuchhalter zur Erfassung von Risiken zum Risiko-Controller mit Steuerungsfunktion. Risikomanager wie sie in der RMA organisiert sind, setzen sich zum Ziel, auf betriebswirtschaftlich fundierter Basis und mit Hilfe geeigneter Methoden die Leitung von Unternehmen und Organisationen beim Erreichen der Unternehmensziele zu unterstützen. Diese Aufgabe des Risikomanagements ist sowohl im US-Standard von COSO zum Enterprise Risk Management als auch in der international anerkannten ISO Norm 31000 kodifiziert.

Durch freiwillige Prüfungen des Risikomanagementsystems i.S.v. IDW EPS 981 werden auch die Risikomanager und deren Aufgabenerfüllung auf den Prüfstand gestellt. Daher haben sie ein berechtigtes Interesse, Stellung zum vorgesehenen neuen Prüfungsstandard zu beziehen.

Durch Mitarbeit an der Neufassung des Revisionsstandards Nr. 2 des DIIR zur Prüfung des Risikomanagements hat sich die RMA aktiv am Standard Setting beteiligt und hat auch an den Konsultationen in der Vorbereitungsphase des IDW zur Erarbeitung des neuen Prüfungsstandards schon die Gelegenheit wahrgenommen, Stellung zu beziehen. Mit dieser Stellungnahme wollen wir dazu beitragen, den IDW EPS 981 an modernen Risikomanagementsystemen zu orientieren, wie sie insbesondere von Unternehmen zu betreiben sind, die im Wettbewerb stehen, systemrelevant sind und/oder besondere Sicherheitsrisiken haben.

Eckpunkte unserer Stellungnahme

1. Hinsichtlich der Rahmenkonzepte lehnt sich der Prüfungsstandard in weiten Teilen an das Modell von COSO ERM 2008 an und berücksichtigt noch nicht die Weiterentwicklung, die von der COSO derzeit diskutiert wird. Schwerpunkt und Struktur des COSO ERM Update 2016 werden sich erheblich verändern und sollten noch im IDW PS 981 eingearbeitet werden (Komponenten- und Prinzipienansatz). Gleichzeitig wird der international anerkannte Standard ISO 31000 nur am Rande erwähnt, obwohl er mittlerweile weit verbreitet ist.

2. Die integrative Ausrichtung moderner Governance-, Risk- und Compliance-Ansätze spiegelt sich im IDW-Prüfungsansatz zu den Governance-Bereichen (IDW 981-983) nicht angemessen wider. Außerdem ist zu beanstanden, dass die Möglichkeit einer Einschränkung des Prüfungsumfangs durch die Geschäftsleitung in IDW EPS 981 vorgesehen ist. Der Geprüfte kann also den Prüfungsumfang unabhängig vom Auftraggeber beeinflussen.

3. Als Prüfungsgegenstand sollte auch die Risikosteuerung als Kernprozess im RMS hinsichtlich der Frage beurteilt werden, ob Steuerungsmaßnahmen in Bezug auf wesentliche Risiken grundsätzlich geeignet erscheinen, Risiken im Sinne der definierten Risikostrategie zu steuern. Daher ist auch das Interne Kontrollsystem in die Prüfung einzubeziehen.

4. Als Prüfungsschwerpunkt sollten die Verfahren der Risikoaggregation stärker in den Vordergrund gerückt werden, weil bestandsbedrohende Entwicklungen (§ 91 AktG) meist aus Kombinationseffekten von Risiken entstehen und „bestandsgefährdende Einzelrisiken" eher die Ausnahme sind. Zudem wird eine quantitative Methodik zur Risikoaggregation, die über die Summierung von Schadenserwartungswerten hinausgeht, in der Praxis häufig vernachlässigt.

Erläuterungen und Verbesserungsvorschläge

1. Rahmenkonzept (Tz. 5 / Anlage 1)

Richtigerweise weist der IDW EPS 981 in Tz. 5 darauf hin, dass das Risikomanagementsystem (RMS) als Corporate Governance System im Gesetz nicht (eindeutig) definiert ist. Allerdings hat sich die Risikomanagement-Literatur in den letzten Jahren sehr intensiv mit der Definition des RMS beschäftigt und mit COSO ERM sowie ISO 31000 liegen mittlerweile weltweit anerkannte Rahmenwerke vor.

In Tz. 5 referenzieren Sie allerdings nur auf COSO ERM und erwähnen ISO 31000 dort nicht explizit, obwohl er heute von vielen Unternehmen als Basisrahmenwerk zugrunde gelegt wird.

RMA-Vorschlag 1: Sie verzichten in Tz. 5 auf die Nennung von COSO ERM und verweisen auf die Anlage 1 oder es werden beide Standards genannt.

Die Tabelle in Anlage 1 unterscheidet allgemeine von spezifischen Rahmenkonzepten und erfasst unter den allgemeinen Rahmenkonzepten neben COSO ERM und ISO 31000 mit dem BS-6079-3:2000 unseres Erachtens einen spezifischen Standard, nämlich für Projektrisikomanagement. Außerdem enthält die Aufzählung mit der ONR 49000 ff. einen Standard, der nur in Österreich verbreitet und von der Bedeutung her in keiner Weise mit COSO ERM und ISO 31000 gleichzusetzen ist.

RMA-Vorschlag 2: ONR 49000 ff und BS-6079-3:2000 sollten unter den spezifischen Rahmenkonzepten aufgeführt werden.

Hinsichtlich der Rahmenkonzepte orientiert sich der Prüfungsstandard inhaltlich in weiten Teilen aus nachvollziehbaren Gründen am Modell von COSO ERM 2008. Wie Ihnen bekannt sein dürfte, hat COSO eine umfassende Überarbeitung des Standards mit einer neu formulierten Zielsetzung, Reduzierung der Komponenten von acht auf fünf und die Einführung von Prinzipien vorgenommen. Der entsprechende Entwurf befindet sich in der Konsultationsphase.

RMA-Vorschlag 3: IDW EPS 981 sollte unbedingt die Überarbeitung des neuen COSO ERM berücksichtigen.

2. Limitierung des Prüfungsumfangs (Tz. 7 und Tz 10 bzw. Tz. 20)

Mit der Beschränkung des Prüfungsgegenstandes auf die Teile des Risikomanagements, die sich mit den strategischen und den operativen Risiken aus der Geschäftstätigkeit in IDW EPS 981 (Tz. 7) auseinandersetzen, geht das IDW nicht auf die zunehmend integrative Ausrichtung von unternehmensweiten Risikomanagementsystemen ein, die richtigerweise eine enge Verzahnung des Risikomanagements mit dem internen Kontrollsystem und dem Compliance-Management-System in den Unternehmen und Organisationen anstreben bzw. schon umgesetzt haben.

Alle großen Wirtschaftsprüfungsgesellschaften empfehlen in Beratungsprojekten zur Einführung oder Optimierung von RMS unisono integrierte Risikomanagement- und interne Kontrollsysteme, auch bekannt unter dem Stichwort „GRC-Systeme" (Governance-Risk-and-Compliance-Systemen). Der vorliegende Prüfungsstandard IDW EPS 981 bzw. die Standardfamilie IDW PS 981-983 vermittelt den Eindruck, dass separate Governance-Elemente „state-of-the-art" seien und fördert damit das teilweise immer noch vorhandene Silodenken in Unternehmen.

RMA-Vorschlag 4: Sollte es bei dieser Drei-Teilung der Governance-Prüfungsstandards bleiben, empfehlen wir eine ergänzende Erläuterung, die den potenziellen Auftraggebern einer Prüfung nach IDW PS 981 transparent macht, dass hiermit keine Prüfung eines unternehmensweiten und integrierten RMS/IKS erfolgt, so dass das Risiko einer Erwartungslücke reduziert wird.

In Tz. 10 wird den gesetzlichen Vertretern des zu prüfenden Unternehmens die Möglichkeit eingeräumt, eine Abgrenzung zu prüfender Teilbereiche vorzunehmen. Eine Einschränkung des Prüfungsgegenstandes sollte nur der Auftraggeber vornehmen können.

RMA-Vorschlag 5: Streichung des zweiten Satzes in Tz. 10 (sowie entsprechende Anpassung in Tz. 20).

3. Prüfungsgegenstand (Tz. 8 und 60)

In Tz. 8 wird klar herausgestellt, dass offenbar die Risikosteuerung nicht Gegenstand der Betrachtung sein soll ("Ziel ist es dagegen nicht, ..."). Hierdurch wird eine Bewertung des (Risiko-)Managements vermieden, was jedoch in gewisser Weise die Sinnhaftigkeit der gesamten Prüfung in Frage stellt, da ein wesentliches Element des RM-Regelkreises fehlt.

Gleichzeitig findet sich in A41 unter den Anhaltspunkten für wesentliche Mängel des RMS im vierten Punkt der Hinweis: „Es gibt Nachweise dafür, dass die implementierten Regelungen der Steuerung von wesentlichen Risiken nicht geeignet oder unwirksam sind." Folglich müssen auch entsprechende Prüfungshandlungen durchgeführt werden.

Auch aus Tz. 60 ergibt sich richtigerweise indirekt die Auseinandersetzung mit der Risikosteuerung und die Anforderung, die Risikosteuerung zu beurteilen.

Beim Risikomanagement werden zukünftige Entwicklungen abgeschätzt und deren mögliche Auswirkungen bewertet. Danach entscheidet das Management über Maßnahmen, die zu ergreifen sind. Zu diesem Zeitpunkt kann die Unternehmensleitung nicht wissen, ob diese Maßnahmen geeignet sind. Folglich kann auch kein Prüfer (zu diesem Zeitpunkt) wissen und beurteilen, ob diese Maßnahmen geeignet sind. Sehr wohl aber kann ein sachverständiger Prüfer des Risikomanagements bewerten, ob diese Maßnahmen zum Prüfungszeitpunkt geeignet erscheinen, ein Risiko im Einklang mit der Risikostrategie zu steuern. Ist zum Prüfungszeitpunkt ein Risiko eingetreten und die Risikosteuerung nachweislich nicht geeignet gewesen, bedeutet dies nicht unmittelbar, dass die zum Risiko-Bewertungszeitpunkt getroffene Steuerungsentscheidung falsch war und das RMS Mängel hatte. Entscheidend ist, dass zum Zeitpunkt der Risikobewertung eine angemessene (Risiko-)Informationsgrundlage im Sinne der Business Judgement Rule gegeben war.

RMA-Vorschlag 6: Im Satz in Tz. 8: „Ziel ist es dagegen nicht..." den Teil ab „und ob einzelne von den gesetzlichen Vertretern...sinnvoll sind." streichen.

4. Prüfungsschwerpunkt Risikoaggregation (Tz. 30 / A23)

Unter den Grundelementen eines RMS wird in Tz. 30 unter den Zielen des RMS gefordert, in der Risikostrategie festzulegen, in welchem Ausmaß unter Berücksichtigung der Risikotragfähigkeit des Unternehmens Risiken eingegangen werden sollen. Diese Festlegung setzt eine Risikoaggregation voraus, die mit geeigneten Verfahren durchzuführen ist. Insbesondere vor dem Hintergrund, dass bestandsbedrohende Entwicklungen i.S.v. § 91 AktG meist aus Kombinationseffekten von Risiken entstehen und „bestandsgefährdende Einzelrisiken" eher die Ausnahme sind, kommt der Risikoaggregation im RMS eine besondere Bedeutung zu.

In A23 ist im vorletzten Absatz allerdings nur davon die Rede, dass es u.U. sachgerecht sei, Verfahren der Risikosimulation einzusetzen, um eine aggregierte Gesamtrisikoposition ermitteln zu können.

Wir halten es für dringend erforderlich klarzustellen, dass eine Gesamtrisikoposition unter Einsatz von Risikosimulationen zu ermitteln ist. Zumindest sollte klargestellt werden, dass eine Summierung von Schadenserwartungswerten kein geeignetes, sachgerechtes Verfahren der Risikoaggregation darstellt.

RMA-Vorschlag 7: in A23, vorletzter Absatz wie folgt zu formulieren: „zur qualitativen Unterstützung der Risikobewertung ist es sachgerecht, Verfahren der Risikosimulation einzusetzen."

5. Sonstige Anmerkungen

Zu Tz. 8 i.V.m. 17 d:

Der Begriff des „wesentlichen Risikos" wird nicht definiert. Die Erläuterungen in Tz. 49 / A37 beziehen sich nur auf „wesentliche Fehler in der RMS-Beschreibung" bzw. „wesentliche Mängel des RMS". Der Begriff der Wesentlichkeit eines Risikos könnte unter Bezugnahme auf die Bedeutung eines solchen Risikos für das Erreichen der Unternehmensziele und die Risikotragfähigkeit des Unternehmens erläutert werden.

Zu Tz. 17 e:

Die Definition von „Risikomanagement" erscheint zu unbestimmt. Wir empfehlen, die Definition des DIIR Revisionsstandards Nr. 2 zu übernehmen: *„Risikomanagement bezeichnet alle Tätigkeiten, die darauf ausgerichtet sind, Risiken frühzeitig und systematisch zu erfassen, zu steuern und zu überwachen, um das Erreichen der Organisationsziele zu gewährleisten. Dies umfasst die nachvollziehbare und regelmäßige Identifikation von Risiken, deren Analyse und Bewertung, die Implementierung geeigneter Risikosteuerungsmaßnahmen und deren Kontrolle sowie die regelmäßige Berichterstattung und die fortlaufende Überwachung der Risiken und der zuvor genannten Prozessschritte."*

Zu Tz. 19:

Es ist empfehlenswert, den Gegenstand der Prüfung des RMS klarer herauszustellen und zu betonen, dass unabhängig von der gewählten Bezeichnung und Abgrenzung im Unternehmen dem RMS alle Managementsysteme zuzuordnen sind, die sich mit Chancen und Gefahren (Risiken) befassen. Diese Klarstellung erscheint notwendig, weil die zentrale Risikomanagementfunktion oft nur eines von vielen Managementsystemen ist, das sich mit Risiken befasst. §91 Absatz 2 AktG spricht allgemeiner von „Überwachungssystem(en)", das der Vorstand einzurichten hat, um bestandsgefährdende Entwicklungen zu erkennen. Daher sind z.B. auch ein Qualitätsmanagementsystem in der Produktion, das Controlling, das Treasury oder die strategische Planung in die Prüfung mit einzubeziehen, da sie sich eben mit Risiken und deren Früherkennung befassen.

Zu Tz. 20:

Aus unserer Sicht sollte klargestellt werden, welche konkreten Ziele das Risikomanagement erfüllen soll (die damit den Prüfungsumfang bestimmen), wobei neben § 91 AktG auch der bisher wenig beachtete § 93 AktG (Business Judgement Rule) relevant ist. Bei der Prüfung der Eignung des RMS ist eben auch zu untersuchen, ob neben den Anforderungen gemäß § 91 AktG („Früherkennung bestandsgefährdender Entwicklungen") die Beachtung von § 93 AktG (Schaffung „angemessener (Risiko)Informationen" für Entscheidungen der Unternehmensführung) gewährleistet wird.

Zu Tz. A 40

Im dritten Punkt der Aufzählung von Fragestellungen wird von „Potenziellem Schadensausmaß" gesprochen. Dies ist insofern inkonsistent, als Risiko zuvor richtigerweise als positive oder negative Auswirkung (von Unsicherheit) definiert wurde.

Zusammenfassung

Insgesamt ist es aus Sicht von Risikomanagern grundsätzlich positiv zu bewerten, dass es mit einer unabhängigen Prüfung durch Wirtschaftsprüfer zu einer Weiterentwicklung des eigenen RMS, aber auch der Risikomanagement-Profession insgesamt kommen kann und mit dem IDW EPS 981 ein Standard entwickelt wurde, der grundsätzlich auch die Risikosteuerung zum Gegenstand hat.

Gleichzeitig sehen wir aber wie dargelegt noch erheblichen Diskussions- und Änderungsbedarf am neuen Prüfungsstandard, damit er modernen RMS gerecht wird, die Risikomanagement nicht als Buchhaltungs-, sondern als Controlling-Aufgabe i.S.v. Steuerung definieren.

Kritisch sehen wir außerdem, dass es mit dem in 2015 durch das DIIR neu gefassten Revisionsstandard Nr. 2 zur Prüfung des Risikomanagements bereits einen Prüfungsstandard gibt, der zumindest in der Sprache, aber auch in Bezug auf Struktur und Grundelementen abweicht. Die Tätigkeit der Internen Revision hinsichtlich der Prüfung des RMS sollte unbedingt im Rahmen einer Prüfung durch Wirtschaftsprüfer angemessen Berücksichtigung finden, um Doppelarbeiten zu vermeiden und eine effiziente Prüfung zu gewährleisten.

Wir hoffen, mit unseren Anmerkungen und konkreten Verbesserungsvorschlägen einen wertvollen Beitrag zur Optimierung des IDW EPS 981 geleistet zu haben und stehen sehr gerne in der Konsultationsphase für die weitere Diskussion zur Verfügung.

An dieser Stelle möchten wir abschließend erwähnen, dass wir uns inhaltlich auch der Ihnen vorliegenden Stellungnahme unserer Beiratsmitglieds Prof. Dr. Werner Gleißner vollumfänglich anschließen.

Nochmals besten Dank für die Möglichkeit der Stellungnahme.

München, 30. September 2016

Mit freundlichen Grüßen

Ralf Kimpel, Vorsitzender des Vorstands der Risk Management Association e.V.