Anlage 1:

Detaillierte Stellungnahme zum IDW Prüfungsstandards „Die Prüfung der Maßnahmen nach § 91 Abs. 2 AktG im Rahmen der Jahresabschlussprüfung gemäß § 317 Abs. 4 HGB“ (IDW EPS 340 n.F.)

Ad 1: Kurzvorstellung RiskNET

- Mit rund 3 Mio. Pageimpression pro Monat und 7.800 Abonnenten ist RiskNET das führende Kompetenzportal rund um das Thema Risk Management
- Die RiskAcademy – als Fortbildungsakademie unter dem Dach von RiskNET – hat seit ihrer Gründung im Jahr 1998 mehr als 20.000 Risikomanager ausgebildet.
- RiskNET kooperiert seit vielen Jahren mit der TÜV Süd Akademie und bietet seit vielen Jahren eine akkreditierte und zertifizierte Ausbildung im Bereich Risk Management an.
- Seit dem Jahr 2009 bietet die Technische Hochschule Deggendorf in Kooperation mit RiskNET und der TÜV Süd Akademie den akkreditierten Masterstudiengang Risiko- und Compliancemanagement (RCM) an.
- Aus RiskNET wurde im Jahr 2005 als „Spin Off“ die Risk Management Association e.V. (RMA) gegründet. Frank Romeike – als geschäftsführender Gesellschafter der RiskNET GmbH – war Gründungsvorstand der RMA und hatte mit der Gründung das Ziel verfolgt, den Reifegrad im Risikomanagement zu entwickeln sowie den Dialog zwischen Unternehmen zu fördern. Heute hat die RMA rund 670 Mitglieder.
- Mit dem RiskNET Summit veranstaltet die RiskNET GmbH seit Jahrzehnten jährlich eine international anerkannte Fachtagung für Praktiker und Wissenschaftler rund um das Thema Risk Management.
- Frank Romeike ist neben seiner Tätigkeit als geschäftsführender Gesellschafter der RiskNET GmbH auch Mitglied des Vorstands der „Gesellschaft für Risikomanagement und Regulierung e.V.“. Der gemeinnützige Verein, hat sich folgende Ziele gesetzt: 1. Förderung der Forschung und Lehre auf allen Gebieten des Risikomanagements und der Regulierung sowie der ganzheitlichen, praxisorientierten Ausbildung von Risikomanagern für den Finanzsektor sowie 2. Förderung des Verständnisses von "Best-Practice-Standards" für Risikomanagement und Regulierung mit dem Ziel eines nachhaltigen und die Gesamtwirtschaft stärkenden Finanzsektors.
- Seit dem Jahr 2010 hat die „Gesellschaft für Risikomanagement und Regulierung e.V.“ bzw. das „Frankfurter Institut für Risikomanagement und Regulierung“ (FIRM) mehr als 36 derartige Projektförderanträge aus rund 20 Universitäten und Hochschulen mit einem Gesamtvolumen von rund 2,3 Mio. Euro gefördert.

Ad 2: Konkrete Empfehlungen zum IDW EPS 340 n.F.

Textziffer 5 (Gliederungspunkt 1):

In Textziffer 5 wird auf die freiwillige Prüfung des Compliance Management Systems nach IDW PS 980, des Risikomanagementsystems nach IDW PS 981, des internen Kontrollsystems des internen und externen Berichtswesens nach IDW PS 982 sowie des Internen Revisionssystems nach IDW PS 983 verwiesen.

Empfehlung: Bei den zitierten IDW-Standards handelt es sich um gesetzlich als „Nichtprüfungsleistungen" definierte und rein kommerzielle IDW-Standards. Der IDW PS 340 sollte sich ausschließlich auf die gesetzlichen Prüfungsleistungen (im Kontext § 91 Abs. 2 AktG im Rahmen der Jahresabschlussprüfung gemäß § 317 Abs. 4 HGB) fokussieren und jegliche kommerzielle Interessen der Wirtschaftsprüfer bzw. prüfungsnahen Beratungsleistungen außen vor halten.

Textziffer 8 (Gliederungspunkt 2):

Die Definition von Risiken im IDW EPS 340 n.F. entspricht weder internationalen Standards noch der „modernen" und in der Praxis weitestgehend etablierten Definition von Risiken, da im Entwurf ausschließlich auf die „Downside"-Risiken abgestellt wird. An dieser Stelle sei verwiesen auf die folgenden internationalen Definitionen:

Definition in der ISO 31000 (2018):

„Risk: effect of uncertainty on objectives. […] An effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats. […]"

Definition aus COSO Enterprise Risk Management (2017)

„Risk: The possibility that events will occur and affect the achievement of strategy and business objectives."

Bereits die MaRisk VA (Mindestanforderungen an das Risikomanagement in Versicherungsunternehmen) folgten – als sogenannte normeninterpretierende Verwaltungsvorschriften – seit dem Jahr 2009 der folgenden Definition des Risikobegriffs:

„Der Risikobegriff ist im Zusammenhang mit den Zielsetzungen zu interpretieren. Es sind sowohl negative als auch positive Zielabweichungen möglich. [...] Dennoch ist es die Ausgabe eines guten Risikomanagementsystems, unternehmerische Chancen und Risiken zu handhaben" [siehe Abschnitt 5 MaRisk VA aus dem Jahr 2009]

Empfehlung: Der Begriff Risiko sollte sich nicht nur auf negative Ziel-/Planabweichungen konzentrieren, sondern einet „modernen“ und international akzeptierten Definition von Risiko folgen und daher auch die „positiven“ Ziel-/Planabweichungen berücksichtigen.

Eine international akzeptierte Definition des Risikobegriffs ist aus unserer Sicht wichtig, da der Abschlussprüfer nach § 317 Abs. 4 HGB bei börsennotierten Aktiengesellschaften im Rahmen der Abschlussprüfung beurteilt, ob der Vorstand die nach § 91 Abs. 2 AktG erforderlichen Maßnahmen in einer geeigneten Form getroffen hat und ob das danach einzurichtende Überwachungssystem seine Aufgaben erfüllen kann. Eine Mehrzahl der börsenorientierten Unternehmen orientiert sich an internationalen Standards bzw. unterliegt einer europäischen Regulierung (siehe Versicherungen bzw. Banken).

Risiko könnte demnach wie folgt definiert werden:

Risiken sind die aus der Unvorhersehbarkeit der Zukunft resultierenden Möglichkeiten, von geplanten Zielwerten abzuweichen. Risiken können daher auch als „Streuung“ um einen Erwartungs- oder Zielwert betrachtet werden. Risiken sind immer nur in direktem Zusammenhang mit der Planung eines Unternehmens zu interpretieren. Mögliche Abweichungen von den geplanten Zielen stellen Risiken dar – und zwar sowohl negative („Gefahren“) wie auch positive Abweichungen („Chancen“).

Begründung: Eine Vernachlässigung der potenziellen positiven Planabweichungen führt zu einer zu pessimistischen Betrachtung des gesamten Risikoumfangs eines Unternehmens. Dies hat erhebliche Auswirkungen in Bezug auf den Abgleich mit der vorhandenen Risikotragfähigkeit. Unabhängig hiervon ist die im Entwurf enthaltene Definition nicht kompatibel zu etablierten internationalen Standards.

Textziffer 8 (Gliederungspunkt 2):

Die Definition von Risikotragfähigkeit ist stark verkürzt und aus unserer Sicht unzureichend, da hier im Wesentlichen das Risikodeckungspotenzial beschrieben wird.

Empfehlung: Orientierung auch hier an internationalen Standards, beispielsweise „ECB Guide to the internal capital adequacy assessment process (ICAAP)“. Insbesondere fehlt in der Definition ein Bezug zum Risikoappetit/Risikoakzeptanz sowie zur definierten Risikostrategie.

Siehe hierzu auch AT 4.1 Risikotragfähigkeit im Rundschreiben 09/2017 (BA) „Mindestanforderungen an das Risikomanagement – MaRisk“ der BaFin:

„[…] Auf der Grundlage des Gesamtrisikoprofils ist sicherzustellen, dass die wesentlichen Risiken des Instituts durch das Risikodeckungspotenzial, unter Berücksichtigung von Risikokonzentrationen, laufend abgedeckt sind und damit die Risikotragfähigkeit gegeben ist.

Das Institut hat einen internen Prozess zur Sicherstellung der Risikotragfähigkeit einzurichten. […] Die Risikotragfähigkeit ist bei der Festlegung der Strategien (AT 4.2) sowie bei deren Anpassung zu

berücksichtigen. Zur Umsetzung der Strategien beziehungsweise zur Gewährleistung der Risikotragfähigkeit sind ferner geeignete Risikosteuerungs- und -controllingprozesse (AT 4.3.2) einzurichten."

Begründung: Die Definition von Risikotragfähigkeit sollte konsistent zu bereits bestehenden Standards sein und insbesondere die wichtigen Themen Risikoappetit/Risikoakzeptanz und Risikostrategie beinhalten.

Textziffer 10: Bestandsgefährdende Entwicklungen

In Textziffer 10 ist formuliert, dass die Auswahl der Methoden zur Bestimmung der Risikotragfähigkeit im Ermessen des Unternehmens liegen und diese sowohl qualitativ als auch quantitativ ausgestaltet sein können.

Die Formulierung ist nicht kompatibel zu internationalen und nationalen Standards. Exemplarisch sei an dieser Stelle der Abschnitt AT 4.1 Risikotragfähigkeit im Rundschreiben 09/2017 (BA) „Mindestanforderungen an das Risikomanagement – MaRisk" der BaFin zitiert:

„[…] Verfügt ein Institut über keine geeigneten Verfahren zur Quantifizierung einzelner Risiken, die in das Risikotragfähigkeitskonzept einbezogen werden sollen, so ist für diese auf der Basis einer Plausibilisierung ein Risikobetrag festzulegen. Die Plausibilisierung kann auf der Basis einer qualifizierten Expertenschätzung durchgeführt werden.

Die Wahl der Methoden und Verfahren zur Beurteilung der Risikotragfähigkeit liegt in der Verantwortung des Instituts. Die den Methoden und Verfahren zugrunde liegenden Annahmen sind nachvollziehbar zu begründen. Die Festlegung wesentlicher Elemente der Risikotragfähigkeitssteuerung sowie wesentlicher zugrunde liegender Annahmen ist von der Geschäftsleitung zu genehmigen. […] Die Stabilität und Konsistenz der Methoden und Verfahren sowie die Aussagekraft der damit ermittelten Risiken sind insofern kritisch zu analysieren."

In diesem Kontext sei darauf hingewiesen, dass die Beurteilung des Risikodeckungspotenzials in Relation zu den aggregierten Risiken immer eine Quantifizierung bedingt.

An dieser Stelle sei auch verwiesen auf Principle 6 im „ECB Guide to the internal capital adequacy assessment process (ICAAP)". Dort ist folgendes klar formuliert: *„The ICAAP is expected to ensure that risks that the institution is or may be exposed to are adequately quantified. The institution is expected to implement risk quantification methodologies that are tailored to its individual circumstances, (i.e. they are expected to be in line with its risk appetite, market expectations, business model, risk profile, size and complexity). […]*

Risks are not expected to be excluded from the assessment because they are difficult to quantify or the relevant data are not available. In such cases, the institution is expected to determine sufficiently conservative risk figures, taking into consideration all relevant information and ensuring adequacy and consistency in its choice of risk quantification methodologies."

Empfehlung:

Die Formulierung sollte sich an bereits etablierten an akzeptierten Standards orientierten. In diesem Kontext ist es wichtig, dass die Methoden in jedem Fall quantitativ ausgestaltet sein müssen, da nur so eine Abschätzung der Risikotragfähigkeit sachgerecht erfolgen kann.

Begründung: Eine qualitative Ausgestaltung schließt eine Bestimmung der Risikotragfähigkeit bzw. Abwägung des Risikodeckungspotenzials mit dem aggregierten Risikoumfang aus.

Textziffer 11: Bestandsgefährdende Entwicklungen

Die Definition der Ursachen einer bestandsgefährdenden Entwicklung in Textziffer 11 ist stark verkürzt und sehr allgemein formuliert. Bestandsgefährdende Entwicklungen dürfen nicht verwechselt werden mit bestandsgefährdenden Risiken.

Empfehlung:

Die Ursachen einer bestandsgefährdenden Entwicklung sollten transparent formuliert werden. Beispielsweise: *„Von einer bestandsgefährdenden Entwicklung kann dann gesprochen werden, wenn eine Situation der Überschuldung oder eine Situation der Zahlungsunfähigkeit für das Unternehmen durch den Eintritt einzelner oder mehrerer Risiken (in Kombination) droht.“*

Textziffer 18: Risikobewertung

Die aktuelle Formulierung ermöglicht auch eine qualitative Bewertung von Risiken. Dies ist in Bezug auf die Themen Risikotragfähigkeit, aggregierter Risikoumfang und Risikodeckungspotenzial kritisch zu bewerten.

Auch hier empfiehlt sich eine Orientierung an internationalen Standards (siehe oben): „The institution is expected to implement risk quantification methodologies that are tailored to its individual circumstances, (i.e. they are expected to be in line with its risk appetite, market expectations, business model, risk profile, size and complexity). […]

Risks are not expected to be excluded from the assessment because they are difficult to quantify or the relevant data are not available. In such cases, the institution is expected to determine sufficiently conservative risk figures, taking into consideration all relevant information and ensuring adequacy and consistency in its choice of risk quantification methodologies.“ (Principle 6 im „ECB Guide to the internal capital adequacy assessment process (ICAAP)“)

Empfehlung:

Der Einschub „auch für nicht quantifizierbare Risiken“ sollte gestrichen werden. Wir schlagen folgende Ergänzung vor:

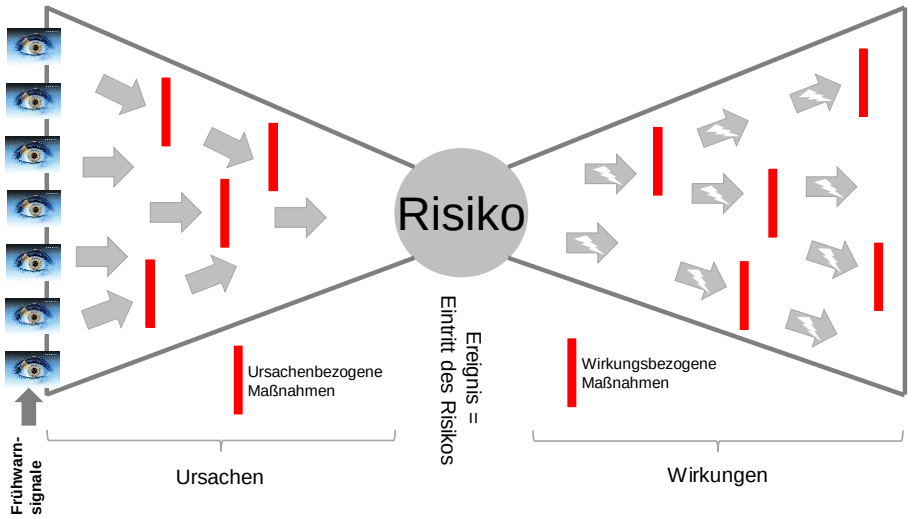
„Risiken sollten nicht von einer quantitativen Bewertung ausgeschlossen werden, weil sie schwer zu quantifizieren sind oder die entsprechenden Daten nicht verfügbar sind. In solchen Fällen wird erwartet, dass das Unternehmen ausreichend konservative Risikoszenarien ermittelt, wobei alle relevanten Informationen berücksichtigt werden und die Angemessenheit und Konsistenz bei der Wahl der Methoden zur Risikoquantifizierung gewährleistet wird.“

Im gesamten Dokument sollte der Begriff „Risikoquantifizierung“ verwenden werden und nicht der Begriff „Risikobewertung“.

Begründung: Eine qualitative Bewertung ermöglicht keine Bewertung eines aggregierten Risikoumfangs in Relation zur Risikotragfähigkeit. Die Möglichkeit einer qualitativen Bewertung ist daher nicht sachgerecht und außerdem nicht konsistent zu vielen internationalen Standards.

Textziffer A3: Definitionen

Unter Textziffer A3 werden eine Reihe von Risiken exemplarisch aufgeführt. Die Aufzählung ist allerdings nicht konsistent, da hier nicht trennscharf zwischen Ursachen, Risiken und Wirkungen unterschieden wird. So ist ein „Verlust betriebsnotwendiger Lizenzen oder Konzessionen“ oder „Betriebsunterbrechungen“ als Ursache (cause) für eine potenzielle Plan-/Zielabweichung zu betrachten. In der Formulierung „Einsatz von spekulativen Finanzinstrumenten, die zur Zahlungsfähigkeit des Unternehmens führen“ ist, wird Ursache (cause), Risiko und Wirkung (effect) miteinander verwoben. Für die Früherkennung von Risiken ist jedoch gerade die saubere Trennung zwischen Ursachen, Risiken und Wirkungen wichtig. Siehe nachfolgende Abbildung:



Empfehlung:

Bei der Definition und exemplarischen Aufzählung sollte methodisch korrekt zwischen Ursachen, Risiken und Wirkungen unterschieden werden.

Textziffer A18:

Hier wird ausgeführt, dass zur Risikoaggregation „einfache Szenarioanalysen" bis hin zu IT-gestützten Simulationsverfahren in Betracht kommen.

Es bleibt unklar, was mit „einfachen" Szenarioanalysen gemeint ist. In jedem Fall ist dies keine korrekte Bezeichnung für eine Methodik. Möglicherweise ist hier eine „deterministische Szenarioanalyse" (vgl. vertiefend Romeike, F./Spitzner, J. (2013): Von Szenarioanalyse bis Wargaming - Betriebswirtschaftliche Simulationen im Praxiseinsatz, Wiley Verlag, Weinheim 2013) gemeint. Fakt ist, dass eine Aggregation von Risiken grundsätzlich nur basierend auf zwei verschiedenen methodischen Ansätzen erfolgen kann.

Die Methodik der „Stochastischen Szenariosimulation" bietet im Risikomanagement einen praktikablen und einfachen Weg, um durch eine Risikoaggregation die Gesamtrisikoposition eines Unternehmens, eines Teilportfolios oder auch eines Projektes zu berechnen und zu analysieren. Außerdem existiert in der Praxis der analytische Weg des Varianz-Kovarianz-Ansatzes an. Das Varianz-Kovarianz-Modell existiert in zwei Varianten, dem Delta-Normal-Ansatz und dem Delta-Gamma-Ansatz. Auf die Normalverteilungshypothese sowie weitere Einschränkung bei der Abwendung soll an dieser Stelle nicht eingegangen werden (vgl. vertiefend Deutsch, H.-P. (2004): Derivate und Interne Modelle – Modernes Risikomanagement, Stuttgart 2004 sowie Romeike, F./Hager, P. (2013): Erfolgsfaktor Risk Management 3.0 – Methoden, Beispiele, Checklisten: Praxishandbuch für Industrie und Handel, 3. Auflage, Wiesbaden 2013.

Empfehlung:

Die Formulierung „einfache Szenarioanalyse" sollten angepasst werden. Es sollten hier lediglich Methoden aufgeführt werden, die tatsächliche eine Aggregation von Risiken ermöglich (Simulationsverfahren bzw. analytische Verfahren, siehe oben).

Besten Dank für die eingeräumte Möglichkeit einer Stellungnahme zu dem von Ihnen veröffentlichten IDW Prüfungsstandards „Die Prüfung der Maßnahmen nach § 91 Abs. 2 AktG im Rahmen der Jahresabschlussprüfung gemäß § 317 Abs. 4 HGB“ (IDW EPS 340 n.F.).

14. Januar 2020

Frank Romeike

Geschäftsführender Gesellschafter

RiskNET GmbH - The Risk Management Network
Ganghoferstr. 43a | D-83098 Brannenburg

E-Mail: office@risknet.de