Dezember 2012

AFRAC

AUSTRIAN FINANCIAL REPORTING AND AUDITING COMMITTEE

Stellungnahme

Beurteilung der Funktionsfähigkeit des Risikomanagements nach Regel 83 des Österreichischen Corporate Governance Kodex

Vorsitzender der Arbeitsgruppe:

Helmut Kerschbaumer (hkerschbaumer@kpmg.at)

Mitglieder der Arbeitsgruppe:

Elfriede Baumann, Michael Eberhartinger, Franz Fischer, Peter Geyer, Michael Heller, Günther Hirschboeck, Christoph Krischanitz, Aslan Milla, Christian Nowotny, Katharina van Bakel-Auer

AFRAC
AUSTRIAN FINANCIAL REPORTING AND AUDITING COMMITTEE

Das Austrian Financial Reporting and Auditing Committee (AFRAC, Beirat für Rechnungslegung und Abschlussprüfung) ist der privat organisierte und von den zuständigen Behörden unterstützte österreichische Standardsetter auf dem Gebiet der Finanzberichterstattung und Abschlussprüfung. Die Mitglieder des Vereins „Österreichisches Rechnungslegungskomitee“, dessen operatives Organ das AFRAC ist, setzen sich aus österreichischen Bundesministerien und offiziellen fachspezifischen Organisationen zusammen. Die Mitglieder des AFRAC sind Abschlussersteller, Wirtschaftsprüfer, Steuerberater, Wissenschaftler, Investoren, Analysten und Mitarbeiter von Aufsichtsbehörden.

Austrian Financial Reporting and Auditing Committee – AFRAC
1120 Wien, Schönbrunner Straße 222–228/1/6
Österreich

Tel: +43 1 811 73 – 228
Fax: +43 1 811 73 – 100
Email: office@afrac.at
Web: http://www.afrac.at

Die vorliegende Stellungnahme basiert auf einem **Diskussionspapier** zur Beurteilung der Funktionsfähigkeit des Risikomanagments nach Regel 83 des Österreichischen Corporate Governance Kodex des **Fachsenats für Unternehmensrecht und Revision** der Kammer der Wirtschaftstreuhänder.

Überblick

1. Zielsetzung und Anwendungsbereich

(1) Gemäß Regel 83 des Österreichischen Corporate Governance Kodex (ÖCGK, Fassung Jänner 2012) hat der Abschlussprüfer auf Grundlage der vorgelegten Dokumente und der zur Verfügung gestellten Unterlagen die Funktionsfähigkeit des Risikomanagements zu beurteilen und dem Vorstand darüber zu berichten. Dieser Bericht ist dem Vorsitzenden des Aufsichtsrats zur Kenntnis zu bringen. Dieser hat Sorge zu tragen, dass der Bericht im Prüfungsausschuss behandelt und im Aufsichtsrat darüber berichtet wird.

(2) Diese Stellungnahme regelt Inhalt und Umfang der Beurteilung der Funktionsfähigkeit des Risikomanagements (im Folgenden: die Beurteilung) durch den Abschlussprüfer, beschreibt die Vorgehensweise bei der Auftragserteilung und gibt Anleitung für die Berichterstattung. Die Durchführung der Beurteilung durch den Abschlussprüfer ist in relevanten nationalen und internationalen Standards (Fachgutachten über die Durchführung von sonstigen Prüfungen des Fachsenats für Unternehmensrecht und Revision des Instituts für Betriebswirtschaft, Steuerrecht und Organisation der Kammer der Wirtschaftstreuhänder [KFS/PG 13[1]] sowie International Standard on Assurance Engagements [ISAE] 3000[2]) geregelt.

(3) Diese Stellungnahme ist auf die Beurteilung bei allen Unternehmen, für die der ÖCGK relevant ist, anzuwenden. Bei der Beurteilung der Funktionsfähigkeit des Risikomanagements von Unternehmen, für die besondere regulatorische Vorschriften gelten (wie Kreditinstitute, Zahlungsinstitute und E-Geld-Institute, Versicherungsunternehmen, Pensionskassen, Mitarbeitervorsorgekassen, Verwaltungsgesellschaften (KAG) von Investmentfonds oder Immobilienfonds, Wertpapierfirmen und Wertpapierdienstleistungsunternehmen), sind die dar-

[1] www.kwt.or.at; KFS/PG 13 – Durchführung von sonstigen Prüfungen.

[2] www.ifac.org; ISAE 3000 – Assurance Engagements Other Than Audits or Reviews of Historical Financial Information.

aus resultierenden branchenspezifischen Anforderungen an das Risikomanagement entsprechend zu berücksichtigen.

2. Gegenstand und Umfang der Beurteilung

2.1. Umfang des Auftrages zur Beurteilung

(4) Die Beurteilung ist eine sonstige Prüfung im Sinne des Fachgutachtens KFS/PG 13. Sonstige Prüfungen im Sinne dieses Fachgutachtens sind Prüfungen mit dem Ziel, ein Urteil darüber abzugeben, ob ein Ist-Objekt mit einem Soll-Objekt (Referenzmodell) übereinstimmt. Das Ergebnis dieser Prüfung wird in Form einer Zusicherung bestätigt.

(5) Die Aufgabe des Abschlussprüfers besteht darin, zu beurteilen, ob im Unternehmen ein angemessenes Risikomanagementsystem eingerichtet ist und ob dieses geeignet ist, effektiv zu sein. Die Beurteilung umfasst dabei die Gestaltung (*Design*) und die Umsetzung (*Implementation*) der wesentlichen Prozesse, Aktivitäten und Kontrollen im Risikomanagement. Die Prüfung der tatsächlichen operativen Wirksamkeit (*Operating Effectiveness*) des Risikomanagements ist nicht Gegenstand der Beurteilung. Ebenso sind die Vollständigkeit der vom Unternehmen tatsächlich identifizierten Risiken und deren zutreffende Bewertung nicht von der Beurteilung durch den Abschlussprüfer umfasst.

2.2. Gegenstand der Beurteilung (Ist-Objekt)

(6) Ist-Objekt ist das im Unternehmen zu einem bestimmten Zeitpunkt eingerichtete Risikomanagement. Mit Unternehmen ist dabei jene börsennotierte Einheit (Konzern, Teilkonzern oder einzelnes Unternehmen) gemeint, die den ÖCGK anwendet. Das Risikomanagement einzelner in einen (Teil-)Konzernabschluss einbezogener Unternehmen (Teilbereiche) ist nicht Prüfungsgegenstand.

(7) Der Zeitpunkt für die Beurteilung ist entweder der Abschlussstichtag oder ein anderer Tag im jeweiligen Berichtsjahr und muss im Auftragsschreiben festgelegt werden.

2.3. Referenzmodell (Soll-Objekt)

(8) Als Referenzmodell dienen allgemein anerkannte Rahmenwerke (Rahmenkonzepte) für ein unternehmensweites Risikomanagementsystem oder – falls ein Unternehmen ein individuell entwickeltes Rahmenwerk (Rahmenkonzept) anwendet – allgemein anerkannte Grundsätze für ein ordnungsgemäßes unternehmensweites Risikomanagementsystem.

(9) Vom Unternehmen individuell entwickelte Rahmenwerke (Rahmenkonzepte) müssen alle für die Funktionsfähigkeit notwendigen Elemente eines allgemein anerkannten Rahmenwerks (Rahmenkonzepts) für ein unternehmensweites Risikomanagementsystem enthalten.

2.4. Zusicherung

(10) Mit der Erteilung einer Zusicherung sichert der Abschlussprüfer den Berichtsadressaten einen entsprechenden Grad an Vertrauen in die grundsätzliche Funktionsfähigkeit des Risikomanagements zu. Das Unternehmen kann mit dem Abschlussprüfer eine auf eine positive oder eine auf eine negative Zusicherung gerichtete Beurteilung vereinbaren.

(11) Falls aufgrund von wesentlichen Feststellungen eine uneingeschränkte Zusicherung nicht möglich ist, hat der Abschlussprüfer die Zusicherung entsprechend zu modifizieren. Die konkrete Formulierung der Modifikation wird vom beauftragten Abschlussprüfer bestimmt.

3. Beauftragung der Beurteilung

3.1. Auftragserteilung

(12) Die Durchführung der Beurteilung ist vom Unternehmen gesondert zu beauftragen. Dies erfolgt entweder durch den Vorstand nach vorheriger Abstimmung mit dem Aufsichtsrat oder durch den Aufsichtsrat.

3.2. Auftragsschreiben

(13) Für den Auftrag zur Beurteilung der Funktionsfähigkeit des Risikomanagements ist ein gesondertes Auftragsschreiben notwendig.

(14) Das Auftragsschreiben sollte folgende Mindestinhalte umfassen:

- Verantwortung des Vorstandes (des zuständigen Vorstandsmitgliedes) für das Risikomanagement
- Art und Umfang der Tätigkeit einschließlich der Feststellung, dass der Umfang ausschließlich die Gestaltung und die Umsetzung, nicht aber die Prüfung der operativen Wirksamkeit des Risikomanagements sowie die Prüfung der Vollständigkeit der vom Unternehmen tatsächlich identifizierten Risiken und der zutreffenden Bewertung der identifizierten Risiken umfasst
- Hinweis auf diese Stellungnahme und zum Referenzmodell sowie eine eindeutige Festlegung, ob die Tätigkeit auf eine positive oder eine negative Zusicherung gerichtet ist
- Stichtag der Beurteilung
- Hinweis, dass die Beurteilung auf Grundlage der vom Unternehmen vorgelegten Dokumente sowie der zur Verfügung gestellten Unterlagen und erteilten Auskünfte erfolgt
- Hinweis auf die Möglichkeit, dass wesentliche Fehler in Abschlüssen, rechtswidrige Handlungen oder andere Verstöße nicht entdeckt werden, weil deren Entdeckung nicht Gegenstand des Auftrages ist
- Hinweis darauf, dass der Beurteilung die Allgemeinen Auftragsbedingungen für Wirtschaftstreuhandberufe in der jeweils geltenden Fassung zugrunde liegen
- Form und Inhalt der Berichterstattung

- Festlegung, ob der Bericht vom Unternehmen an Dritte weitergegeben werden darf
- Feststellung, dass der Abschlussprüfer vom Vorstand eine schriftliche Erklärung einholen wird, dass die vom Unternehmen vorgelegten Unterlagen und erteilten Auskünfte das Risikomanagement vollständig abbilden
- die Vereinbarung über das Honorar

4. Berichterstattung

(15) Die Berichterstattung des Abschlussprüfers erfolgt in schriftlicher Form gegenüber dem in Regel 83 des ÖCGK in der jeweils gültigen Fassung vorgesehenen bzw. gegenüber dem im Auftragsschreiben festgelegten Adressaten.

(16) Die Berichterstattung hat folgende Mindestinhalte zu enthalten:

- Auftraggeber und/oder Berichtsadressat(en)
- Überschrift, die klar zum Ausdruck bringt, ob es sich um die Erteilung einer positiven oder einer negativen Zusicherung zur Gestaltung und Umsetzung des Risikomanagements des geprüften Unternehmens handelt
- Stichtag der Beurteilung
- Hinweis auf die Berufsgrundsätze, nach denen der Auftrag abgewickelt wurde
- Hinweis auf die Verantwortlichkeiten des Vorstandes und des beauftragten Abschlussprüfers in Bezug auf das Risikomanagement und dessen Beurteilung
- zusammenfassende Beschreibung des Auftragsumfanges sowie der im Rahmen des Auftrages durchgeführten für die Beurteilung relevanten Tätigkeiten

- Hinweis, dass die operative Wirksamkeit des Risikomanagements sowie die Vollständigkeit der vom Unternehmen tatsächlich identifizierten Risiken und deren zutreffende Bewertung nicht Gegenstand der Beurteilung waren und daher dazu keine Aussagen getroffen werden können
- Beschreibung der vom Unternehmen vorgelegten Dokumente und der zur Verfügung gestellten Unterlagen, die Nachweise für das vom Unternehmen eingerichtete Risikomanagement (Ist-Objekt) geben
- kurze Darstellung der vom Unternehmen verwendeten allgemein anerkannten Grundsätze für ein ordnungsgemäßes unternehmensweites Risikomanagementsystem oder Verweis auf das vom Unternehmen angewendete allgemein anerkannte Rahmenwerk (Rahmenkonzept)
- Wenn dem Abschlussprüfer im Rahmen seiner Beurteilung der Funktionsfähigkeit des Risikomanagements bekannt geworden ist, dass das Risikomanagement vom Unternehmen während des Geschäftsjahres geändert wurde, so ist dieser Umstand gesondert zu berichten.
- Wenn dem Abschlussprüfer im Rahmen seiner Prüfungshandlungen Umstände bekannt geworden sind, die auf eine wesentliche Schwäche im Risikomanagement hinweisen, so ist darüber gesondert zu berichten.
- Ergebnis der durchgeführten Tätigkeiten des Abschlussprüfers

  Eine positive Zusicherung soll folgendermaßen lauten: „Nach meiner/unserer Beurteilung aufgrund der von mir/uns im Rahmen der durchgeführten Tätigkeiten gewonnenen Erkenntnisse ist das vom Unternehmen eingerichtete Risikomanagement zum … (Stichtag), gemessen am oben beschriebenen Referenzmodell, funktionsfähig."

  Eine negative Zusicherung soll folgendermaßen lauten: „Aufgrund der von mir/uns im Rahmen der durchgeführten Tätigkeiten gewonnenen

Erkenntnisse sind mir/uns keine Sachverhalte bekannt, die mich/uns zu der Annahme veranlassen, dass das vom Unternehmen eingerichtete Risikomanagement zum … (Stichtag), gemessen am oben beschriebenen Referenzmodell, nicht funktionsfähig ist."

Wenn der Abschlussprüfer im Rahmen seiner Beurteilung der Funktionsfähigkeit des Risikomanagements zum Ergebnis kommt, dass die Funktionsfähigkeit des eingerichteten Risikomanagements nur eingeschränkt oder nicht gegeben ist, hat er diesen Umstand in seiner Zusicherung zum Ausdruck zu bringen.

- Verweis auf die Geltung der Allgemeinen Auftragsbedingungen für Wirtschaftstreuhandberufe in der jeweils geltenden Fassung

(17) Der Bericht ist mit jenem Datum zu unterfertigen, an dem die Beurteilung abgeschlossen wurde.

5. Erstmalige Anwendung

(18) Diese Stellungnahme ist für Aufträge über Beurteilungen im Zusammenhang mit der Abschlussprüfung von Geschäftsjahren, die nach dem 30. Juni 2013 enden, anzuwenden. Eine frühere Anwendung wird empfohlen.

Anhang: Grundlagen der Schlussfolgerungen

Zu Rz 1:

Die Fassung des ÖCGK vom Jänner 2012 beinhaltet wie die vorangegangenen Fassungen die Comply or Explain-Regel (C-Regel) über die Beurteilung der Funktionsfähigkeit des Risikomanagements des Unternehmens durch den Abschlussprüfer.

In den Interpretationen zum ÖCGK (Fassung Jänner 2012) erläutert der Österreichische Arbeitskreis für Corporate Governance Inhalt und Umfang dieser Beurteilung näher und stellt unter anderem fest, dass

- die Beurteilung über die bloße Stellungnahme zu Risiken und Empfehlungen im internen Kontrollsystem, wie sie üblicherweise in der Kommunikation zwischen Abschlussprüfer und Aufsichtsrat oder Vorstand Gegenstand sein können, hinausgeht;
- die Nachvollziehbarkeit der Risikoidentifikation und -beschreibung auf Basis der zur Verfügung gestellten Unterlagen sowie die ausreichende Dokumentation des Risikomanagementsystems durch das Unternehmen notwendige Voraussetzungen für die Durchführung der Beurteilung mit vertretbarem Aufwand darstellen;
- Form und Inhalt der Berichterstattung einer gesonderten Vereinbarung unterliegen;
- zur Beurteilung zunächst die im Unternehmen eingesetzten Systeme und Einrichtungen (Risikomanagementmethoden, Sicherungsstrategien, Methoden und Systeme zur Identifikation, Erfassung, Analyse, Bewertung, Kontrollen und Kommunikation der Risiken im Unternehmen etc.) zu erheben sind und sich der Abschlussprüfer über die Wirksamkeit der Maßnahmen und organisatorischen Vorkehrungen sowie Kontrollen durch entsprechende Stichproben zu vergewissern hat;
- zur Definition der Begriffe „Risiko“ und „Risikomanagement“ auf internationale Vorbilder und Modelle zurückgegriffen werden kann.

Auf Grund der zum Teil unklaren Abgrenzung des Begriffs „Risikomanagement“ und der schwierigen Einordnung der Beurteilung in die so genannten Assurance-Leistungen von Wirtschaftstreuhändern („Prüfung“, „Sonstige Prüfungen“, „Vereinbarte Prüfungshandlungen“) war eine unterschiedliche Vorgehensweise bei der Durchführung solcher Beurteilungen und der Berichterstattung darüber zu beobachten. Darüber hinaus bestand das Risiko, dass der tatsächliche Umfang der durchgeführten Beurteilung von den Berichtsadressaten unzutreffend (vor allem als zu weitreichend) interpretiert wird („Erwartungslücke“).

Zu Rz 2:

Zielsetzungen der Stellungnahme sind die Definition des Umfangs der Beurteilung, die Regelung der Auftragserteilung und der Berichterstattung über die Beurteilung, die Einordnung der Beurteilung in die bestehenden Assurance-Leistungen von Wirtschaftstreuhändern sowie die Regelung von einzelnen für diese Beurteilung spezifischen Fragen. Die Basis dafür bildet die Regel 83 des ÖCGK unter Berücksichtigung der dazugehörigen vom Österreichischen Arbeitskreis für Corporate Governance herausgegebenen Interpretation. Diese umfasst auch die Vorgabe, dass eine solche Beurteilung mit vertretbarem Aufwand – d.h. einem ausgewogenen Verhältnis zwischen Kosten und Nutzen – durchzuführen ist.

Die an den Wirtschaftstreuhänder gerichteten konkreten Richtlinien zur Durchführung der Beurteilung im Sinne einer Zusicherungsleistung sind in nationalen und internationalen Standards enthalten (Fachgutachten KFS/PG 13 des Fachsenats für Unternehmensrecht und Revision der Kammer der Wirtschaftstreuhänder über die Durchführung von sonstigen Prüfungen[3] sowie International Standard on Assurance Engagements (ISAE) 3000[4]). Aus diesem Grund enthält diese Stellungnahme keine Richtlinien für die Durchführung der Beurteilung.

Zu Rz 3:

Das Risikomanagement von Unternehmen, die besonderen regulatorischen Vorschriften unterliegen (vor allem Banken, Versicherungs- und Finanzdienstleistungsunternehmen), unterscheidet sich in den konzeptionellen Grundsätzen (Erfassung, Beurteilung, Quantifizierung und Aggregation, Steuerung und Überwachung der Risiken) nicht wesentlich von dem der übrigen Unternehmen. Risikomanagement wird auch für diese Unternehmen als „stetiger Prozess zur Schaffung von Transparenz und Risikominimierung“ verstanden (s.a. OeNB-Leitfadenreihe zum Kreditrisiko, Kreditvergabeprozess und Kreditrisikomanagement, 2004, S. 56). Durch die einschlägigen Materiengesetze (wie BWG, VAG, WAG u.a.) werden spezifische Vorgaben, Prozesse und Verfahren normiert, die die Einrichtung eines Risikomanagements und von Kontrollmechanismen erfordern, welche nach der Art, dem Umfang und der Komplexität der betriebenen Geschäfte angemessen einzurichten sind. Beispielsweise werden Risikokategorien angeführt, die besonders zu berücksichtigen sind (wie in § 39 BWG), oder die Einrichtung von Verfahren und Prozessen gefordert, welche die frühzeitige Erkennung von Risikopotentialen und die Einrichtung von Absicherungs- und Risikoabwehrmechanismen und eine die Organisationseinheiten übergreifende Risikobetrachtung gewährleisten (wie in § 17b VAG).

---

[3] www.kwt.or.at; KFS/PG 13 – Durchführung von sonstigen Prüfungen.

[4] www.ifac.org; ISAE 3000 – Assurance Engagements Other Than Audits or Reviews of Historical Financial Information.

Zu Rz 4:

Die vom ÖCGK definierten Ansprüche an die Beurteilung erfüllen die Tatbestandsmerkmale einer sonstigen Prüfung gemäß KFS/PG 13.

Zu Rz 5:

Eine vollständige Prüfung von Kontrollsystemen nach internationalen Prüfungsgrundsätzen umfasst die Beurteilung der Gestaltung der Kontrollen (*Design*), die Prüfung, ob diese Kontrollen im Unternehmen tatsächlich umgesetzt sind (*Implementation*), sowie die Prüfung, ob sie auch ordnungsgemäß ausgeführt werden (*Operating Effectiveness*). Rz 5 stellt klar, dass die Beurteilung ausschließlich „*Design*“ und „*Implementation*“ umfasst. Sie beinhaltet daher eine Beurteilung der wesentlichen Aktivitäten, Prozesse und Kontrollen des Risikomanagements im Hinblick darauf,

(a) ob sie so gestaltet sind, dass sie grundsätzlich für ein funktionsfähiges Risikomanagement geeignet sind, und

(b) ob diese Aktivitäten, Prozesse und Kontrollen auch konzernweit umgesetzt sind.

Sie umfasst nicht die Prüfung, ob diese Aktivitäten, Prozesse und Kontrollen auch tatsächlich in der vorgesehenen Weise ausgeführt werden, also im Unternehmen operativ wirksam sind. Die Prüfungshandlungen des Abschlussprüfers bestehen daher im Wesentlichen aus dem Lesen der bestehenden dokumentierten Beschreibungen des Risikomanagements (z.B. des Risikomanagement-Handbuchs), der Beurteilung, ob dieses Risikomanagement die wesentlichen Anforderungen an ein funktionierendes Risikomanagement erfüllt, der Befragung von mit dem Risikomanagement befassten Personen, dem Nachvollziehen einzelner wesentlicher Prozesse anhand von Dokumenten (ein so genannter Walk-Through) und der Durchsicht der wesentlichen dokumentierten Ergebnisse des Risikomanagements (z.B. von Risikoberichten). Die Prüfungshandlungen enthalten keine detaillierte Prüfung der Funktionsfähigkeit einzelner Prozesse und Kontrollen, beispielsweise auf Grundlage von für eine Prüfung der *Operating Effectiveness* erforderlichen statistisch relevanten Stichproben.

Die Prüfung der „*Operating Effectiveness*“ würde über die Zielsetzung des ÖCGK hinausgehen, was daraus abgeleitet werden kann, dass die Regel 83 nur eine Beurteilung auf Basis der zur Verfügung gestellten Unterlagen fordert und dass die Beurteilung mit vertretbarem Aufwand durchgeführt werden soll. Die Prüfung und Bestätigung der ordnungsgemäßen Ausführung (*Operating Effectiveness*) würde einen erheblich größeren Zeit- und damit Kostenaufwand bedeuten. Eine so weit gefasste Prüfpflicht ist auch für die durch das URÄG 2008 eingeführten Angaben im Lagebericht im Zusammenhang mit den wichtigsten Merkmalen des internen Kontroll- und des Risikomanagementsystems im Hinblick auf den Rechnungslegungsprozess nicht vorgesehen (vgl. Erläuternde Bemerkungen zum URÄG 2008).

Selbstverständlich steht es dem Auftraggeber (Vorstand bzw. Aufsichtsrat, vgl. Rz 12) frei, eine über den beschriebenen Umfang hinausgehende Beurteilung, die auch die Prüfung der Operating Effectiveness umfasst, zu beauftragen.

Die Vollständigkeit der vom Unternehmen tatsächlich identifizierten Risiken ist für den Abschlussprüfer faktisch nicht überprüfbar, weil für die Vollständigkeitsprüfung von Risiken keine substantiellen Prüfungshandlungen möglich sind. Der Abschlussprüfer kann nur beurteilen, ob Aktivitäten, Prozesse und Kontrollen bestehen, die ausreichend sicherstellen, dass die Unternehmensleitung alle wesentlichen Risiken tatsächlich erkennen und entsprechende Maßnahmen ergreifen kann. Dies entspricht dem Verständnis der Prüfung des Risikomanagements als Prozessprüfung.

Stellt der Abschlussprüfer fest, dass das Unternehmen wesentliche Risiken nicht erkannt und berichtet hat, weist dies auf mögliche Schwächen im Risikomanagement hin.

Zu Rz 6:

Der ÖCGK richtet sich vorrangig an österreichische börsennotierte Unternehmen. Damit ist jene rechtliche Einheit gemeint, die den Kapitalmarkt in Anspruch nimmt. Die Beurteilung des Risikomanagements umfasst die wirtschaftlichen Einheiten, die dem beherrschenden Einfluss dieser rechtlichen Einheit unterliegen. Mit anderen Worten: Gegenstand der Beurteilung ist nicht nur das Risikomanagement der Muttergesellschaft, sondern jenes des gesamten Konzerns. Dies ergibt sich einerseits aus der Tatsache, dass auch die Finanzberichterstattung den gesamten Konzern umfasst, anderseits aber auch daraus, dass die Risiken einer Muttergesellschaft sehr eng mit jenen der von ihr beherrschten Tochtergesellschaften verbunden sind. Ist die börsenotierte Muttergesellschaft selbst in einen übergeordneten Konzern einbezogen, so unterliegt der von der börsenotierten Muttergesellschaft gebildete Teilkonzern der Beurteilung. Denkbar ist auch der Fall, dass die börsennotierte Gesellschaft ein einzelnes Unternehmen darstellt.

Im Falle eines Konzerns umfasst die Beurteilung das konzernweite Risikomanagement und nicht jenes einzelner Tochtergesellschaften (Teilbereiche), weil für den Aufsichtsrat und die Teilnehmer am Kapitalmarkt i.d.R. der Konzern insgesamt und nicht einzelne Tochtergesellschaften isoliert relevant sind. Dies schließt nicht aus, dass der Abschlussprüfer im Rahmen der Beurteilung des konzernweiten Risikomanagements auch dessen Umsetzung in einzelnen Tochtergesellschaften prüfen muss.

Zu Rz 7:

Die Beurteilung der Gestaltung und der Umsetzung eines Systems ist typischerweise zeitpunktbezogen. Bei einer zeitraumbezogenen Beurteilung der Gestaltung und der Umsetzung wären statistisch relevante Stichproben notwendig, um eine Aussage bzgl. der Funktionsfähigkeit über diese gesamte Periode hinweg treffen zu können, was zu einem wesentlich höheren Prüfungsaufwand führen würde.

Der Abschlussprüfer soll im Zuge der Beurteilung allerdings hinterfragen, ob in einer bestimmten Periode (i.d.R. einem Geschäftsjahr) wesentliche Änderungen im Risikomanagement stattgefunden haben, und darüber berichten (vgl. Rz 16).

Regel 83 des ÖCGK legt keinen Stichtag fest. Damit steht dem Auftraggeber die Wahl eines Stichtages im jeweiligen Berichtsjahr offen.

Zu Rz 8:

Zur objektiven Beurteilung der Funktionsfähigkeit des Risikomanagements ist es erforderlich, das im Unternehmen eingerichtete Risikomanagement (Prüfungsgegenstand, Ist-Objekt) an Hand eines Referenzmodells (Soll-Objekt) zu beurteilen. Sowohl die Interpretationen zu Regel 83 des ÖCGK als auch die Erläuternden Bemerkungen zu § 92 Abs. 4a AktG i.d.F. der Regierungsvorlage des URÄG 2008 sowie die AFRAC-Stellungnahme zur Lageberichterstattung gemäß §§ 243, 243a und 267 UGB (Rz 60) enthalten den Hinweis, dass für dieses Referenzmodell auf internationale Vorbilder und Modelle zurückgegriffen werden kann. Das vom Committee of Sponsoring Organizations of the Treadway Commission (COSO)[5] herausgegebene Rahmenwerk (Rahmenkonzept) stellt ein in der Praxis häufig angewendetes Rahmenwerk (Rahmenkonzept) dar. Andere in Frage kommende Rahmenwerke (Rahmenkonzepte) sind beispielsweise ONR[6] 49000ff („Risikomanagement für Organisationen und Systeme“), ONR S2410 („Chancen- und Risikomanagement“) sowie branchen- und aufgabenspezifische Rahmenwerke (Rahmenkonzepte).

Unternehmen können ihr Risikomanagement auch nach individuell entwickelten Rahmenwerken (Rahmenkonzepten) gestalten. In diesem Fall dienen die allgemein anerkannten Grundsätze für ein unternehmensweites Risikomanagementsystem als Referenzmodell. Nach diesen Grundsätzen muss ein unternehmensweites Risikomanagementsystem folgende Eigenschaften aufweisen und folgende Elemente enthalten:

- **Nachhaltigkeit und gesamtheitliche Betrachtung:** Ein funktionsfähiges Risikomanagement erfordert einen permanenten, die gesamte Organisation (alle Organisationseinheiten, Abteilungen, (Tochter-)Unternehmen) umfassenden Prozess.
- **Angemessenheit:** Das eingerichtete Risikomanagementsystem hat in seiner Ausgestaltung der Größe und Komplexität des Unternehmens Rechnung zu tragen.
- **Commitment:** Ein funktionsfähiges Risikomanagement setzt eine Verankerung in der Unternehmenskultur und somit die Mitwirkung jedes Mitarbeiters im Unternehmen voraus und muss vom Management unterstützt werden.

---

[5] http://www.coso.org

[6] Standard des österreichischen Normungsinstituts; URL: http://www.as-search.at/publish/home.html

- **Objektivität:** Die Risikoeinschätzungen müssen objektivierbar und nachvollziehbar gestaltet sein.
- **Integration:** Die Risikobeurteilungen müssen in den Unternehmensalltag und in die Unternehmenssteuerung einfließen, insbesondere auch in die Planung.
- **Validierung und laufende Verbesserung:** Das Risikomanagementsystem muss laufend auf Validität und Konsistenz seiner Ergebnisse überprüft und regelmäßig aktualisiert, verfeinert und verbessert werden.
- **Angemessene Sicherheit:** Das Risikomanagementsystem muss geeignet sein, alle relevanten Ereignisse zu identifizieren, die die Erreichung der Unternehmensziele wesentlich beeinflussen können.

Um diese Grundvoraussetzungen im Unternehmen operationalisieren zu können, sind folgende überprüfbare organisatorische Elemente erforderlich:

- **Risikodefinition:** Ist der Risikobegriff im Unternehmen klar definiert und jedem bekannt?
- **Verantwortung:** Bestehen klare Verantwortungen für die Umsetzung des Risikomanagements?
- **Risikomanagementprozess:** Ist ein Risikomanagementprozess eingerichtet (Risikoidentifikations-, Risikobewertungs- und Risikosteuerungsprozesse)?
- **Risikobewertung:** Ist die Logik der Bewertung nachvollziehbar und ist die Bedeutung des Risikowertes (Risikokennzahl) klar? Sind Risikokennzahlen und Steuerungskennzahlen aufeinander abgestimmt? Wird die Bewertung von Personen mit ausreichender Fachkenntnis und Erfahrung durchgeführt?
- **Risikosteuerung:** Werden auf Basis der identifizierten Risiken angemessene Maßnahmen zur Risikosteuerung (z.B. Risikovermeidung, Risikoreduktion, Riskoverlagerung oder Risikoakzeptanz) definiert und umgesetzt?
- **Risikobericht:** Besteht ein angemessener Risikobericht? Enthält er alle relevanten Informationen? Erfolgt die Verteilung an die zuständigen Personen? Erfolgt eine regelmäßige Berichterstattung an Leitungs- und Aufsichtsorgane?
- **Überwachung:** Wird die Funktionsfähigkeit des eingerichteten Risikomanagementsystems laufend überwacht und werden etwaige auftretende Schwächen behoben?

Auf europäischer Ebene werden im Rahmen der Capital Requirements Directive (CRD) IV, welche u. a. die Beaufsichtigung von Kreditinstituten und Wertpapierfirmen regelt, zur Stärkung der Corporate Governance Maßnahmen mit dem Ziel, die Wirksamkeit der Risikobeherrschung zu stärken, vorgeschrieben. Als zu beachtende Kriterien für ein wirksames Risikomanagement führt die CRD IV beispielsweise an, dass dieses (i) dauerhaft eingerichtet ist, (ii) von den operativen Einheiten hierarchisch

und funktionell unabhängig ist, (iii) dem Risikoprofil des Gesamtunternehmens angemessen ist, (iv) mit entsprechender maßgeblicher Kompetenz in Bezug auf das Risiko-Reporting und den strategischen Risikomanagement-Entscheidungsprozess ausgestattet ist, (v) einer ständigen Weiterentwicklung und Anpassung an sich verändernde Geschäftsmodelle unterliegt, (vi) eine die Risikopolitik beeinflussende Vergütungsregelung des Managements berücksichtigt und (vii) ordnungsmäßig dokumentiert ist (Risikohandbuch) (siehe hierzu die Begründung zu Corporate Governance und Art. 75 im Vorschlag der Europäischen Kommission für CRD IV, Stand 20. Juli 2011).

Zu Rz 10:

Bei sonstigen Prüfungen kann die Zusicherung entweder positiv oder negativ formuliert sein (vgl. KFS/PG 13, Rz 24). Mit den beiden Aussagen wird dem Berichtsadressaten ein unterschiedlicher Grad an Vertrauen in die Erfüllung bzw. Einhaltung der für den Auftragsgegenstand maßgebenden Vorgaben zugesichert. Die positive Zusicherung ist mit einem höheren Prüfungsaufwand verbunden. Die negative Zusicherung geht mit einem geringeren Umfang an vorzunehmenden Prüfungshandlungen zur Einholung von Nachweisen einher, weshalb die Risiken einer Fehlbeurteilung höher sind als bei einer positiven Zusicherung (vgl. KFS/PG 13, Rz 41). Regel 83 des ÖCGK enthält keine Aussage, ob die Beurteilung des Abschlussprüfers in Form einer positiven oder einer negativen Zusicherung (Bestätigung) erfolgen soll. Daher obliegt es dem Auftraggeber, bei der Auftragserteilung die gewünschte Form der Zusicherung festzulegen.

Zu Rz 11:

Die Entscheidung darüber, ob eine Modifizierung erforderlich ist, und deren Ausgestaltung richten sich nach den für die Durchführung von sonstigen Prüfungen geltenden nationalen und internationalen Standards (vgl. Grundlagen der Schlussfolgerungen zu Rz 2).

Zu Rz 12:

Weder die Regel 83 des ÖCGK noch die dazugehörige Interpretation legen fest, wer auf Seite des Unternehmens die Durchführung der Beurteilung zu beauftragen hat. Eine Beauftragung durch den Vorstand als für die Gesellschaft vertretungsbefugtes Organ ist jedenfalls möglich. Eine Abstimmung mit dem Aufsichtsrat ist in diesem Fall zu empfehlen, weil der Bericht über die Beurteilung dem Vorsitzenden des Aufsichtsrats zur Kenntnis zu bringen ist. Gemäß § 95 Abs. 3 AktG kann der Aufsichtsrat für bestimmte Aufgaben besondere Sachverständige beauftragen, weshalb auch eine Beauftragung der Prüfung des Risikomanagementsystems durch den Aufsichtsrat möglich ist.

Zu Rz 13:

Verträge zwischen geprüftem Unternehmen und Abschlussprüfer unterliegen aufgrund nationaler und internationaler Regeln der Schriftform. Dies soll auch für den Auftrag zur Beurteilung gelten. Die Prüfung der Funktionsfähigkeit des Risikomanagements ist in keiner Weise einer Jahresabschlussprüfung

gleichzustellen, da sich Art und Umfang der Prüfung unterscheiden. Deshalb ist ein eigenes Auftragsschreiben erforderlich.

Zu Rz 14:

Der Inhalt des Auftragsschreibens richtet sich nach den für Assurance-Leistungen von Wirtschaftstreuhändern üblichen Grundsätzen.

Die Beurteilung erfolgt auf Grundlage der vorgelegten Dokumente und zur Verfügung gestellten Unterlagen bzw. Auskünfte, sodass der bei Prüfungsaufträgen übliche Satz über den uneingeschränkten Zugang zu Informationen und Auskünften entfallen kann. Hat der Aufsichtsrat jedoch eine Prüfung beauftragt, die über den in der Regel 83 ÖCGK vorgesehenen Prüfungsumfang hinaus eine Beurteilung der operativen Wirksamkeit des Risikomanagementsystems (*Operating Effectiveness*) umfasst, hat die Unternehmensleitung auch eine qualitative Aussage über die Wirksamkeit des Risikomanagements zu tätigen („*Self Assessment*"). Dies ist im Auftragsschreiben festzuhalten.

Die vom Arbeitskreis für Honorarfragen und Auftragsbedingungen der Kammer der Wirtschaftstreuhänder festgestellten und regelmäßig adaptierten sowie vom Vorstand der Kammer der Wirtschaftstreuhänder mit Beschluss vom 8. März 2000 zur Anwendung empfohlenen Allgemeinen Auftragsbedingungen für Wirtschaftstreuhandberufe finden für vergleichbare Leistungen von Wirtschaftstreuhändern Anwendung. Ihre Anwendung ist auch für Beurteilungen sinnvoll.

Zu Rz 15:

Die Berichterstattung hat gemäß der Regel 83 des ÖCGK (in der jeweils gültigen Fassung) zu erfolgen.

Zur eindeutigen Dokumentation des Inhalts der Berichterstattung muss diese in schriftlicher Form erfolgen. Die Wahl des Formates („klassisches" Berichtsformat oder Präsentationsformat) obliegt dem beauftragten Abschlussprüfer.

Zu Rz 16:

Der Inhalt der Berichterstattung folgt den für Assurance-Leistungen von Wirtschaftstreuhändern üblichen Grundsätzen.