Dezember 2020

AFRAC

AUSTRIAN FINANCIAL REPORTING AND AUDITING COMMITTEE

AFRAC-Stellungnahme 19

Funktionsfähigkeit Risikomanagement (ÖCGK)

Stellungnahme

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

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

Zitiervorschlag:

Kurzzitat: AFRAC 19 (Dezember 2020), Rz ...

Langzitat: AFRAC-Stellungnahme 19: Funktionsfähigkeit Risikomanagement (ÖCGK) (Dezember 2020), Rz ...

AFRAC
AUSTRIAN FINANCIAL REPORTING AND AUDITING COMMITTEE

Historie der vorliegenden Stellungnahme

erstmalige Veröffentlichung	Dezember 2012	
Überarbeitung	Dezember 2015	nur formale Anpassung; bis auf geringfügige Aktualisierungen keine inhaltlichen Änderungen
Überarbeitung	Dezember 2020	Anpassung aufgrund der Änderungen von KFS/PG 13 und ISAE 3000; sonst keine wesentlichen inhaltlichen Änderungen

AFRAC
AUSTRIAN FINANCIAL REPORTING AND AUDITING COMMITTEE

Die vorliegende Stellungnahme basiert auf einem Diskussionspapier zur Beurteilung der Funktionsfähigkeit des Risikomanagements nach Regel 83 des Österreichischen Corporate Governance Kodex des Fachsenats für Unternehmensrecht und Revision der Kammer der Wirtschaftstreuhänder (nunmehr: Kammer der Steuerberater und Wirtschaftsprüfer).

AUSTRIAN FINANCIAL REPORTING AND AUDITING COMMITTEE

Inhaltsverzeichnis

1. Zielsetzung und Anwendungsbereich 5

2. Umfang, Gegenstand und Kriterien der Beurteilung 7

2.1. Umfang des Auftrages 7

2.2. Gegenstand der Beurteilung (zugrunde liegender Sachverhalt) 7

2.3. Referenzmodell (geeignete Kriterien) 8

2.4. Zusammenfassende Beurteilung 8

3. Beauftragung der Beurteilung 9

3.1. Auftragserteilung 9

3.2. Auftragsschreiben 9

4. Berichterstattung 10

5. Erstmalige Anwendung 13

Erläuterungen 14

1. Zielsetzung und Anwendungsbereich

(1) Gemäß Regel 83 des Österreichischen Corporate Governance Kodex (ÖCGK, Fassung Jänner 2020) 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: „Beurteilung“) durch den Abschlussprüfer, beschreibt die Vorgehensweise bei der Auftragserteilung und gibt Anleitung für die Berichterstattung. Die Durchführung der Beurteilung durch den Abschlussprüfer ist im Fachgutachten KFS/PG 13 (Durchführung von sonstigen Prüfungen) des Fachsenats für Unternehmensrecht und Revision des Instituts für Betriebswirtschaft, Steuerrecht und Organisation der Kammer der Steuerberater und Wirtschaftsprüfer geregelt. In diesem Fachgutachten sind die wesentlichen Aussagen des International Standard on Assurance Engagements (ISAE) 3000 Revised – Assurance Engagements Other than Audits or Reviews of Historical Financial Information berücksichtigt.

(3) Diese Stellungnahme ist für alle Unternehmen und deren Abschlussprüfer relevant, die ein Bekenntnis zum ÖCGK abgegeben haben. Bei der Beurteilung der Funktionsfähigkeit des Risikomanagements von Unternehmen, für die besondere regulatorische Vorschriften gelten (wie Kreditinstitute, Zahlungsinstitute und E-Geld-Institute, Versicherungsunternehmen, Pensionskassen, Betriebliche Vorsorgekassen, Verwaltungsgesellschaften (OGAW) von Investmentfonds oder Immobilienfonds, Wertpapierfirmen und Wertpapierdienstleistungsunternehmen), sind die daraus resultierenden branchenspezifischen Anforderungen an das Risikomanagement entsprechend zu berücksichtigen.

2. Umfang, Gegenstand und Kriterien der Beurteilung

2.1. Umfang des Auftrages

(4) Die Beurteilung der Funktionsfähigkeit des Risikomanagements durch den Abschlussprüfer stellt i.d.R. einen direkten Zusicherungsauftrag (*direct engagement*) im Sinne des Fachgutachtens KFS/PG 13 dar. Die Aufgabe des Abschlussprüfers besteht darin, anhand eines Referenzmodells (geeigneter Kriterien) zu beurteilen, ob das Unternehmen ein funktionsfähiges Risikomanagement eingerichtet hat (zugrunde liegender Sachverhalt). Unter Risikomanagement sind dabei jene von der Unternehmensleitung getroffenen organisatorischen Vorkehrungen und Maßnahmen zu verstehen, die sicherstellen sollen, dass wesentliche strategische, finanzielle und operative Risiken sowie Risiken von Regelverstößen eines Unternehmens rechtzeitig identifiziert, bewertet, gesteuert und überwacht werden.

(5) Die Beurteilung umfasst 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 (zugrunde liegender Sachverhalt)

(6) Gegenstand der Beurteilung (der zugrunde liegende Sachverhalt) ist das im Unternehmen zum Zeitpunkt der Beurteilung eingerichtete Risikomanagement. Mit Unternehmen ist dabei jene börsenotierte 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 (geeignete Kriterien)

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

(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. Zusammenfassende Beurteilung

(10) Mit der zusammenfassenden Beurteilung sichert der Abschlussprüfer den Berichtsadressaten einen entsprechenden Grad an Vertrauen in die Funktionsfähigkeit des Risikomanagements zu. Für die Beurteilung im Sinne von Regel 83 des ÖCGK ist eine Prüfung mit begrenzter Sicherheit ausreichend. Bei einer Prüfung mit begrenzter Sicherheit erfolgt die zusammenfassende Beurteilung in einer Form, bei der der Abschlussprüfer auf Grundlage der durchgeführten Prüfungshandlungen und erlangten Nachweise urteilt, dass ihm keine Sachverhalte bekannt geworden sind, die ihn zu der Auffassung gelangen lassen, dass das vom Unternehmen eingerichtete Risikomanagement zum … [Stichtag], gemessen am oben beschriebenen Referenzmodell, nicht funktionsfähig ist (negative Zusicherung).

(11) Falls aufgrund von wesentlichen Feststellungen eine uneingeschränkte Zusicherung nicht möglich ist, hat der Abschlussprüfer die Zusicherung entsprechend zu modifizieren.

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 einer Bezugnahme auf diese Stellungnahme sowie auf das Fachgutachten KFS/PG 13
- eine eindeutige Festlegung, dass die Tätigkeit auf eine Beurteilung mit begrenzter Sicherheit gerichtet ist
- die 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 das Referenzmodell (geeignete Kriterien)
- 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 selbst wesentliche Fehler, rechtswidrige Handlungen oder andere Verstöße möglicherweise nicht entdeckt werden, weil deren Entdeckung nicht Gegenstand des Auftrages ist
- Hinweis, dass dem Auftrag subsidiär die AAB für WT-Berufe i.d.g.F. zugrunde liegen; sie sollten dem Auftragsbestätigungsschreiben beigelegt werden
- 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 allenfalls zusätzlich im Auftragsschreiben festgelegten Adressaten.

(16) Die Berichterstattung hat folgende Mindestinhalte zu enthalten:

- Überschrift, die klar zum Ausdruck bringt, dass es sich um eine Berichterstattung über eine unabhängige Prüfung handelt
- Auftraggeber und/oder Berichtsadressat(en)
- Berufsgrundsätze, nach denen der Auftrag abgewickelt wurde, und die dem Auftrag zugrunde gelegten AAB für WT-Berufe i.d.g.F. sowie eine

Erklärung, dass der beauftragte Abschlussprüfer die Anforderungen an die Unabhängigkeit und sonstige berufliche Verhaltensanforderungen einhält

– Identifizierung des Stichtags der Beurteilung und Beschreibung des vom beauftragten Abschlussprüfer erlangten Niveaus an Prüfungssicherheit; 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 (den zugrunde liegenden Sachverhalt) geben; wenn dem Abschlussprüfer im Rahmen der Beurteilung bekannt geworden ist, dass das Risikomanagement vom Unternehmen während des Geschäftsjahres geändert wurde, so ist dieser Umstand gesondert zu berichten

– Identifizierung der anzuwendenden Kriterien (Angabe des Rahmenkonzepts oder kurze Darstellung der vom Unternehmen verwendeten allgemein anerkannten Grundsätze für ein ordnungsgemäßes unternehmensweites Risikomanagementsystem)

– Beschreibung der signifikanten inhärenten Beschränkungen, die mit der Beurteilung des Risikomanagements anhand der anzuwendenden Kriterien zusammenhängen; es kann sich beispielsweise als sinnvoll erweisen anzumerken, dass vergangene Beurteilungen des Risikomanagementsystems für zukünftige Perioden nicht relevant sind, weil das Risiko besteht, dass interne Kontrollen unangemessen werden, weil sich die Bedingungen geändert haben

- Hinweis, ob der Bericht neben einer Behandlung im Prüfungsausschuss und der Berichterstattung im Aufsichtsrat vom Unternehmen an Dritte weitergegeben werden darf
- Hinweis auf die Verantwortlichkeiten des Vorstandes und des beauftragten Abschlussprüfers in Bezug auf das Risikomanagement und dessen Beurteilung
- Erklärung, dass der Auftrag in Übereinstimmung mit dieser Stellungnahme und dem Fachgutachten KFS/PG 13 durchgeführt wurde
- eine informative Zusammenfassung der durchgeführten Tätigkeiten zur Vermittlung eines Verständnisses von Art, zeitlicher Einteilung und Umfang der durchgeführten Prüfungshandlungen
- Ergebnis der durchgeführten Tätigkeiten des Abschlussprüfers

  Die zusammenfassende Beurteilung auf Basis einer begrenzten Sicherheit hat folgendermaßen zu lauten: „Auf Grundlage der durchgeführten Prüfungshandlungen und erlangten Nachweise sind uns keine Sachverhalte bekannt geworden, die uns zu der Auffassung gelangen lassen, 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 zusammenfassenden Beurteilung zum Ausdruck zu bringen.
- 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.

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

5. Erstmalige Anwendung

(18) Die vorliegende Fassung der Stellungnahme ersetzt jene vom Dezember 2015. Sie ist für Aufträge über Beurteilungen im Zusammenhang mit der Abschlussprüfung von Geschäftsjahren, die nach dem 31. Dezember 2020 enden, anzuwenden. Eine frühere Anwendung wird empfohlen.

Erläuterungen

Zu Rz (1):

Die Fassung des ÖCGK vom Jänner 2020 beinhaltet wie die vorangegangenen Fassungen die Comply or Explain-Regel (C-Regel) 83 über die Beurteilung der Funktionsfähigkeit des Risikomanagements des Unternehmens durch den Abschlussprüfer („Regel 83 des ÖCGK“).

In den Interpretationen zum ÖCGK (Fassung Februar 2018) erläutert der Österreichische Arbeitskreis für Corporate Governance Inhalt und Umfang dieser Beurteilung näher und stellt 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;
- die Beurteilung mit vertretbarem Aufwand – d.h. einem ausgewogenen Verhältnis zwischen Kosten und Nutzen – durchzuführen ist;
- 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.

Aufgrund der zum Teil unklaren Abgrenzung des Begriffs „Risikomanagement“ und der schwierigen Einordnung der Beurteilung in die verschiedenen Leistungen von Wirtschaftstreuhändern („Prüfungen“, „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 Einordnung der Beurteilung in das Regelwerk für Zusicherungsleistungen von Wirtschaftsprüfern, die Definition des Umfangs der Beurteilung, die Regelung der Auftragserteilung und der Berichterstattung über die Beurteilung 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.

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 des Instituts für Betriebswirtschaft, Steuerrecht und Organisation der Kammer der Steuerberater und Wirtschaftsprüfer über die Durchführung von sonstigen Prüfungen sowie International Standard on Assurance Engagements (ISAE) 3000 Revised).

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. Beispielsweise finden sich in den EBA-Leitlinien zur internen Governance, Abschnitt 17, entsprechende Beschreibungen für ein Risikomanagement-Rahmenwerk bei Kreditinstituten. 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 zu gestalten 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 Risikopotenzialen und die Einrichtung von Absicherungs- und Risikoabwehrmechanismen und eine die Organisationseinheiten übergreifende Risikobetrachtung gewährleisten (wie in § 17b Abs. 5 VAG; ähnlich, aber umfassender § 110 VAG 2016).

Zu Rz (4):

Die vom ÖCGK definierten Ansprüche an die Beurteilung erfüllen die Tatbestandsmerkmale einer sonstigen Prüfung gemäß dem Fachgutachten KFS/PG 13. Sonstige Prüfungen sind auftragsgebundene Prüfungen, bei denen entweder eine andere Partei als der beauftragte Wirtschaftsprüfer den zugrunde liegenden Sachverhalt anhand von Kriterien misst oder beurteilt und der beauftragte Wirtschaftsprüfer

zu dieser Information eine zusammenfassende Beurteilung (*conclusion*) abgibt (*attestation engagements*, Attestierungsaufträge) oder der beauftragte Wirtschaftsprüfer den zugrunde liegenden Sachverhalt unmittelbar anhand von Kriterien selbst misst oder beurteilt (*direct engagements*, direkte Zusicherungsaufträge) (vgl. KFS PG/13 Rz 5).

Das in einem Unternehmen eingerichtete Risikomanagementsystem stellt den zugrunde liegenden Sachverhalt dar, welcher anhand geeigneter Kriterien zu beurteilen ist. Die daraus resultierende Sachverhaltsinformationen (Aussage über die Funktionsfähigkeit des Risikomanagementsystems) ist Bestandteil der zusammenfassenden Beurteilung durch den Abschlussprüfer.

Die Beurteilung stellt nach herrschender Praxis einen direkten Zusicherungsauftrag dar, weil der beauftragte Abschlussprüfer die Beurteilung des Risikomanagements i.d.R. unmittelbar anhand der geeigneten Kriterien selbst vornimmt.

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,

(b) ob sie der unternehmensweiten Situation entsprechend aktualisiert worden sind und

(c) 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 in einem bestimmten Zeitraum 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 des ÖCGK nur eine Beurteilung der Funktionsfähigkeit 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). Der Auftraggeber kann jedoch eine über den beschriebenen Umfang hinausgehende Beurteilung 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 börsenotierte Unternehmen. Damit ist jene rechtliche Einheit gemeint, die den Kapitalmarkt in Anspruch nimmt. Die Beurteilung umfasst auch jene wirtschaftlichen Einheiten, die dem beherrschenden Einfluss dieser rechtlichen Einheit unterliegen. Gegenstand der Beurteilung ist daher 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 börsenotierte 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 (*Design*) und der Umsetzung (*Implementation*) 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 für die Beurteilung fest. Damit steht dem Auftraggeber die Wahl eines Stichtages im jeweiligen Berichtsjahr offen.

Zu Rz (8):

Zur objektiven Beurteilung ist es erforderlich, das im Unternehmen eingerichtete Risikomanagement (Prüfungsgegenstand, zugrunde liegender Sachverhalt) an Hand eines Referenzmodells (geeigneter Kriterien) 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 Rz 60 der AFRAC-Stellungnahme 9 „Lageberichterstattung gemäß §§ 243 bis 243b, 267 und 267a UGB“ 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, http://www.coso.org) herausgegebene Rahmenwerk (Rahmenkonzept) – 2017 Enterprise Risk Management – Integrating with Strategy and Performance – und ihre Vorgänger-Versionen stellen ein in der Praxis häufig angewendetes Rahmenwerk (Rahmenkonzept) dar. Andere in Frage kommende Rahmenwerke (Rahmenkonzepte) sind beispielsweise ÖNORM (Standard des österreichischen Normungsinstituts) D 4900 („Risikomanagement für Organisationen und Systeme – Begriffe und Grundlagen – Anleitung zur Umsetzung der ISO 31000“), ISO 31000:2018 (Risk Management – Guidelines) und ISO 31010:2019 (Risk Management – Risk Assessment Techniques). Darüber hinaus bestehen branchen- und aufgabenspezifische Rahmenwerke (Rahmenkonzepte).

Für Kreditinstitute beinhaltet z.B. Art. 76 der Capital Requirements Directive (CRD) IV, welche u.a. die Beaufsichtigung von Kreditinstituten und Wertpapierfirmen regelt, Anforderungen an die „Behandlung

von Risiken“. Verbindliche Vorgaben zur Ausgestaltung des Risikomanagements finden sich in der nationalen Umsetzung der CRD IV im BWG (§ 39, Allgemeine Sorgfaltspflichten) sowie in der Kreditinstitute-Risikomanagementverordnung (KI-RMV). § 3 der KI-RMV enthält eine Aufzählung der allgemeinen Prinzipien für das Risikomanagement bei Kreditinstituten.

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

- Risikomanagement-Organisation
- Risikostrategie
- Risikoidentifikation und -erfassung
- Risikoanalyse und -bewertung
- Risikosteuerung und -überwachung
- Risikoberichterstattung und Kommunikation

Das unternehmensweite Risikomanagement muss dabei folgende Eigenschaften aufweisen:

- 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.
- 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 (strategische) Planung und die Performancemessung.
- 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 Merkmale erforderlich:

- Risikodefinition und -strategie: Ist der Risikobegriff im Unternehmen klar definiert und jedem bekannt? Ist festgelegt, in welchem Ausmaß unter Berücksichtigung der Risikotragfähigkeit des Unternehmens Risiken eingegangen werden sollen (Risikoappetit)?
- Verantwortung: Bestehen klare Verantwortlichkeiten 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 und eines definierten Risikoappetits angemessene Maßnahmen zur Risikosteuerung (z.B. Risikovermeidung, Risikoreduktion, Risikoverlagerung 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?

Zu Rz (10):

Eine sonstige Prüfung kann entweder eine Prüfung mit hinreichender Sicherheit oder eine Prüfung mit begrenzter Sicherheit sein bzw. eine Kombination beider (vgl. KFS/PG 13 Rz 34 ff.).

Eine Prüfung mit begrenzter Sicherheit liegt vor, wenn der beauftragte Abschlussprüfer als Grundlage für die Abgabe einer zusammenfassenden Beurteilung das Auftragsrisiko auf ein Maß reduziert, das unter den Umständen des Auftrages vertretbar, aber höher ist als bei einer Prüfung mit hinreichender Sicherheit. Die zusammenfassende Beurteilung erfolgt in Form einer negativen Zusicherung. Dabei ist die zusammenfassende Beurteilung so formuliert, dass sie vermittelt, ob auf Grundlage der durchgeführten Prüfungshandlungen und der erlangten Nachweise Sachverhalte bekannt geworden sind, die den beauftragten Abschlussprüfer zur Auffassung gelangen lassen, dass die Funktionsfähigkeit des vom Unternehmen eingerichteten Risikomanagements nicht (ausreichend) gegeben ist.

Eine Prüfung mit hinreichender Sicherheit verringert das Auftragsrisiko auf ein gegenüber einer Prüfung mit begrenzter Sicherheit niedrigeres Maß und ist daher auch mit einem höheren Prüfungsaufwand verbunden. Die Berichterstattung enthält eine zusammenfassende Beurteilung über das Ergebnis der Prüfung des zugrunde liegenden Sachverhalts anhand der Kriterien (positive Zusicherung).

Regel 83 des ÖCGK enthält keine Aussage darüber, ob die Beurteilung des Abschlussprüfers mit hinreichender oder begrenzter Sicherheit erfolgen soll. Die vom Österreichischen Arbeitskreis für Corporate Governance herausgegebenen Interpretationen (vgl. die Erläuterungen zu Rz (1)), vor allem die Schlussfolgerung, dass die Beurteilung mit vertretbarem Aufwand und einem ausgewogenen Verhältnis zwischen Kosten und Nutzen durchzuführen ist, deuten darauf hin, dass eine Prüfung mit begrenzter Sicherheit i.d.R. als ausreichend angesehen wird. Es obliegt 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. die Erläuterungen zu Rz (2)).

Zu Rz (12):

Weder die Regel 83 des ÖCGK noch die dazugehörige Interpretation legen eindeutig fest, wer auf Seite des Unternehmens die Durchführung der Beurteilung zu beauftragen hat. Da die Berichterstattung jedenfalls gegenüber dem Vorstand zu erfolgen hat, ist eine Beauftragung durch diesen als für die Gesellschaft vertretungsbefugtes Organ 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 und dieser Sorge zu tragen hat, dass der Bericht im Prüfungsausschuss behandelt und im Aufsichtsrat darüber berichtet wird. 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) und (14):

Verträge zwischen geprüftem Unternehmen und Abschlussprüfer unterliegen üblicherweise und aufgrund internationaler Regeln der Schriftform. Dies soll auch für den Auftrag zur Beurteilung gelten. Der Inhalt des Auftragsschreibens richtet sich nach den für sonstige Prüfungen 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 Vorstand oder Aufsichtsrat jedoch eine

Prüfung mit hinreichender Sicherheit beauftragt, muss der Abschlussprüfer uneingeschränkten Zugang zu Informationen und Auskünften erhalten. Dies ist im Auftragsschreiben festzuhalten.

Die von der Kammer der Steuerberater und Wirtschaftsprüfer festgestellten und regelmäßig adaptierten sowie vom Vorstand der Kammer der Steuerberater und Wirtschaftsprüfer 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 sonstige Prüfungen üblichen Grundsätzen.