04.19

54. Jahrgang
August 2019
Seiten 145–196

www.ZIRdigital.de

ZIR

Zeitschrift Interne Revision

Fachzeitschrift für Wissenschaft und Praxis

Herausgeber:
DIIR Deutsches Institut für Interne Revision e.V.

ESV ERICH SCHMIDT VERLAG

20380

PROF. DR. WERNER GLEISSNER · RALF KIMPEL

Prüfung des Risikomanagements und der neue DIIR Revisionsstandard Nr. 2

Anforderungen der §§91 und 93 AktG an das Risikomanagement im Fokus

Prof. Dr. Werner Gleißner
ist Vorstand der Future-Value Group AG, Honorarprofessor an der TU Dresden und Mitglied im gemeinsamen DIIR- und RMA-Arbeitskreis „Interne Revision und Risikomanagement".
Ralf Kimpel,
CIA CRMA, ist Vorsitzender des Vorstands der Risk Management Association e. V. (RMA) und Leiter des Arbeitskreises „Interne Revision und Risikomanagement".

Die Anforderungen an das Risikomanagement haben sich seit Inkrafttreten des KonTraG (1998) deutlich verändert. Diesen Veränderungen wird der Ende 2018 veröffentlichte neue DIIR Revisionsstandard Nr. 2 gerecht. Neue Anforderungen an das Risikomanagement (zum Beispiel infolge § 93 AktG mit seinen Implikationen für entscheidungsvorbereitende Risikoanalyse) werden ebenso betrachtet wie ältere aus § 91 AktG. So wird die gesetzliche Kernanforderung aus § 91 AktG – frühe Erkennung möglicher bestandsgefährdender Entwicklungen – zum Prüfungsschwerpunkt (zum Beispiel die Risikoaggregationsmodelle, die nötig sind, um bestandsgefährdende Entwicklungen aus Kombinationseffekten von Einzelrisiken zu erkennen). Der DIIR Revisionsstandard Nr. 2 unterscheidet erstmals die Prüfung von (1) Organisation und Prozessen und (2) betriebswirtschaftlichen Methoden (zum Beispiel zur Risikoquantifizierung und Risikoaggregation).

1. Vorbemerkung: Die Prüfung des Risikomanagements und der neue DIIR Revisionsstandard Nr. 2

Das Risikomanagement, speziell das Risikofrüherkennungssystem, ist ein besonders wesentlicher Prüfungsgegenstand für die Interne Revision und Thema des neuen DIIR Revisionsstandards Nr. 2. Bei einer nicht sicher vorhersehbaren Zukunft mit einer Vielzahl von Chancen und Gefahren (Risiken) sind die Fähigkeiten eines Unternehmens im Umgang mit Risiken, speziell bei der Vorbereitung wesentlicher unternehmerischer Entscheidungen, von hoher Bedeutung für den Unternehmenserfolg. Als Mindestanforderung fordert zudem der Gesetzgeber mit § 91 (2) AktG, dass mögliche bestandsgefährdende Entwicklungen früh erkannt werden müssen. Die Interne Revision muss daher insbesondere untersuchen, ob solche bestandsgefährdenden Entwicklungen, die sich im Allgemeinen aus Kombinationseffekten von Einzelrisiken ergeben, tatsächlich erkannt werden können. Auf diese Frage sollte die Prüfaktivität einen klaren Fokus legen. Und entsprechend müssen insbesondere die Methoden für die Risikoaggregation betrachtet werden, die für die Analyse von Kombinationseffekten der Einzelrisiken und zur Beurteilung des Gesamtrisikoumfangs (Eigenkapitalbedarfs) erforderlich sind. Der überarbeitete DIIR Revisionsstandard Nr. 2 (November 2018) hilft bei der Ausgestaltung der Prüfung von Risikomanagementsystemen.

2. Problemstellung und Inhaltsübersicht

In diesem Beitrag werden der DIIR Revisionsstandard Nr. 2 vorgestellt und besonders wesentliche Ansatzpunkte und Fragestellungen für die Prüfung von Risikomanagementsystemen, inklusive eines Checklistensystems, das die Prüfungsanforderungen in nützlicher Weise konkretisiert, knapp zusammengefasst. Ein Fokus liegt dabei auf der Fragestellung, ob durch das Risikofrüherkennungssystem tatsächlich bestandsgefährdende Entwicklungen erkannt werden können, da dies – und nur dies – die zentrale gesetzliche An-

forderung aus § 91 AktG darstellt. Für viele Unternehmen ist zudem noch relativ neu, dass sich aus § 93 AktG wesentliche Implikationen für das Risikomanagement ergeben: Dort wird nämlich gefordert, dass bei der Vorbereitung unternehmerischer Entscheidungen – beweisbar – angemessene Informationen vorgelegen haben müssen. Und in Anbetracht unsicherer Auswirkungen unternehmerischer Entscheidungen[1] bedeutet dies, auch entsprechend den Präzisierungen in der Rechtsprechung,[2] dass insbesondere gezeigt werden muss, welche Veränderungen der Risikoposition mit einer Entscheidung einhergehen. Dies erfordert ein entscheidungsorientiertes Risikomanagement, dessen Risikoanalysen schon bei der Vorbereitung unternehmerischer Entscheidungen einfließen.[3]

Mit dem neuen Prüfungsstandard des DIIR vom November 2018 liegt nun erstmalig ein Standard vor, der die Anforderungen aus § 91 und § 93 AktG gemeinsam betrachtet. Er ist klar auf die Erfüllung der gesetzlichen Kernanforderungen fokussiert (wie die frühe Identifikation möglicher bestandsgefährdender Entwicklungen). Der gelungene und nützliche Standard – sowie die Hintergründe und seine Entwicklung – werden in diesem Beitrag vorgestellt. Die Anwendung des DIIR Revisionsstandard Nr. 2 durch die Interne Revision (oder auch Wirtschaftsprüfer, denen ein vergleichbarer Standard noch fehlt) kann wesentlich dazu beitragen, bestehende Lücken im Risikomanagement beziehungsweise Verbesserungspotenziale aufzudecken und der Geschäftsleitung die Assurance geben, dass ein wirksames Risikomanagementsystem etabliert ist. Dies ist in vielen Unternehmen auch notwendig.[4] Leider zeigt die Praxis, dass bei der Prüfung von Risikomanagementsystemen durch die Interne Revision oder den externen Wirtschaftsprüfer oft vielfältige Aspekte eines Risikomanagementsystems betrachtet werden, ohne dass das gesetzliche Kernthema adäquat gewürdigt wird (vgl. dazu Kapitel drei).

3. Gesetzliche Grundlagen zum Risikomanagement: §§ 91 und 93 AktG

Der Start für die Entwicklung der Risikomanagementsysteme in Deutschland ist das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) aus 1998. Im § 91 (2) AktG steht seitdem: „Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden."

Auf das KonTraG bezieht sich schon seit 1998 das Institut der Wirtschaftsprüfer (IDW). Im PS 340 wird der § 317 (4) konkretisiert und das IDW führt aus, was die Anforderungen an ein Risikofrüherkennungssystem sind. Dort liest man insbesondere (Tz. 10): „Die Risikoanalyse beinhaltet eine Beurteilung der Tragweite der erkannten Risiken in Bezug auf Eintrittswahrscheinlichkeit und quantitative Auswirkungen. Hierzu gehört auch die Einschätzung, ob Einzelrisiken, die isoliert betrachtet von nachrangiger Bedeutung sind, sich in ihrem Zusammenwirken oder durch Kumulation im Zeitablauf zu einem bestandsgefährdenden Risiko aggregieren können."

> **Erforderlich ist ein entscheidungsorientiertes Risikomanagement, dessen Analysen schon bei der Vorbereitung unternehmerischer Entscheidungen einfließen.**

Diese Forderung zur Risikoaggregation ist die zentrale Anforderung an ein Risikomanagementsystem (RMS). Die bestandsgefährdenden Entwicklungen ergeben sich nämlich meist aus Kombinationseffekten von Einzelrisiken, die durch die Risikoaggregation analysiert werden. Da Risiken nicht addierbar sind, benötigt man für die Aggregation eine Monte-Carlo-Simulation.[5]

Bestandsgefährdende Entwicklungen entstehen heute primär durch (drohende) Illiquidität, womit die alleinige Betrachtung der Möglichkeit einer Überschuldung (und bilanzieller Verluste), wie vor Jahren noch üblich, völlig unzureichend ist. Eine drohende Illiquidität ergibt sich in möglichen Zukunftsszenarien, die eine Verletzung von Mindestanforderungen an das Rating zeigen oder bei denen Covenants verletzt werden, die zu einer Kreditkündigung führen. Die Identifikation möglicher bestandsgefährdender Entwicklungen impliziert also die Aggregation von Risiken mit Bezug auf die Unternehmensplanung unter Auswertung

1 Unternehmerische Entscheidungen sind Entscheidungen unter Risiko bzw. Unsicherheit.
2 Siehe Risk Management Association e.V. (2019).
3 Siehe dazu Gleißner, W. (2015) und (2018a).
4 Wie eine Vielzahl empirischer Studien zeigt, siehe z.B. Berger, T./Gleißner, W. (2007); Link, M./Scheffler, R./Oehmann, D. (2018).
5 Siehe Füser, K./Gleißner, W./Meier, G. (1999) und Gleißner, W. (2017a).

der Auswirkungen für Rating und Covenants (und nicht nur durch Überschuldung).

Nach Inkrafttreten des KonTraG (und zum Teil sogar noch heute) war es üblich, in Geschäftsberichten anzugeben, dass es keine bestandsgefährdenden Entwicklungen gäbe. Tatsächlich ist eine derartige Aussage in einer solchen Absolutheit immer falsch, weil es – wenn auch mit geringer Wahrscheinlichkeit – durch irgendeine Kombination von Risiken immer zu einer bestandsgefährdenden Entwicklung kommen kann.[6] Notwendig ist entsprechend eine Angabe über die Wahrscheinlichkeit einer bestandsgefährdenden Entwicklung oder – etwas vereinfacht – die Insolvenzwahrscheinlichkeit. Heute kann man die durch ein Rating ausdrückbare Insolvenzwahrscheinlichkeit als Spitzenkennzahl des Risikomanagements auffassen. Sie drückt die Bedrohungslage des Unternehmens, also den Grad der Bestandsgefährdung aus.[7] Sie ist eine Kennzahl für die interne Steuerung und nicht notwendigerweise zu veröffentlichen.[8]

Das KonTraG zielte zunächst primär auf die Schaffung von Transparenz über bestandsgefährdende Entwicklungen aus Einzelrisiken oder Kombinationseffekten von Einzelrisiken. Spätestens mit der davon unabhängigen Überarbeitung von § 93 AktG (Business Judgement Rule) wurde der Fokus von bestehenden Risiken auf Risiken erweitert, die durch eine unternehmerische Entscheidung (zum Beispiel Investition oder Akquisition) zusätzlich eingegangen werden.

Der Entscheidungsprozess muss sich an geeigneten betriebswirtschaftlichen Methoden der Entscheidungslehre orientieren.

Die Business Judgement Rule – aus § 93 (1) Satz 2 AktG abgeleitet – regelt schadensersatzträchtige Pflichtverletzungen des Vorstands oder Aufsichtsrats (siehe auch § 116 AktG).[9] Grundsätzlich liegt eine Pflichtverletzung dann nicht vor, wenn ein Vorstandsmitglied „bei einer unternehmerischen Entscheidung vernünftigerweise annehmen durfte, auf der Grundlage angemessener Information zum Wohle der Gesellschaft zu handeln." Damit also die Business Judgement Rule greift, muss im Rahmen einer unternehmerischen Entscheidung zwischen alternativen Handlungsmöglichkeiten gewählt werden und die Entscheidung bestimmte Eigenschaften aufweisen. Graumann erläutert: „Dazu gehören nach Auffassung des BGH geeignete Ziele sowie das Abwägen der Vor- und Nachteile der in Betracht kommenden Handlungsmöglichkeiten. Letzteres erfordert Prognosen, wie sich die Handlungsmöglichkeiten auswirken, und dass die damit verbundenen Risiken gemessen und beurteilt werden […]."[10]

Der Entscheidungsprozess muss sich an geeigneten betriebswirtschaftlichen Methoden der Entscheidungslehre orientieren. Bei einer Entscheidung unter Unsicherheit sind es insbesondere die Risikoinformationen, die bei der Entscheidungsvorbereitung wesentlich sind und der Geschäftsführung zur Verfügung gestellt werden müssen, damit diese über angemessene Informationen im Sinne von § 93 (1) Satz 2 AktG verfügt.

Eine Implikation der Business Judgement Rule ist eine Ausweitung des Aufgabenfelds des Risikomanagements. War es mit dem KonTraG 1998 noch akzeptabel, sich nur mit den wesentlichen Risiken zu befassen, die alleine oder in Kombination mit anderen zu bestandsgefährdenden Entwicklungen führen, ist dies inzwischen nicht mehr ausreichend. Durch die Vorgabe von § 93 AktG mit der Forderung nach angemessenen Informationen bei der Entscheidungsvorbereitung ist klar, dass auch die mit der Entscheidung verbundenen Verlustrisiken zu betrachten sind – unabhängig davon, ob diese zu einer bestandsgefährdenden Entwicklung führen können oder nicht. Entscheidungsvorbereitende Risikoanalysen sind damit nun bei allen unternehmerischen Entscheidungen notwendig, die für das Unternehmen so wichtig sind, dass sie vom Vorstand beziehungsweise der Geschäftsführung getroffen werden. Abbildung 2 stellt ein Ablaufdiagramm für den Risikoanalyse- und Bewertungsprozess dar.

Die Unsicherheit über die Zukunftsentwicklung ist die wesentliche Herausforderung der Unternehmensführung im Allgemeinen und der Entscheidungsfindung im Besonderen. Notwendig sind insbesondere leistungsfähige Verfahren für Risikoanalyse, simulationsbasierte Risi-

6 Siehe dazu Gleißner, W. (2017b) und (2017e).

7 Es ist dabei allerdings zu beachten, dass die Insolvenzwahrscheinlichkeit unter Beachtung der Ergebnisse einer Risikoaggregation zu bestimmen ist und nicht lediglich basierend auf (historischen) Finanzkennzahlen, in denen sich nur die in der Vergangenheit realisierten Risiken widerspiegeln (siehe dazu Blum/Gleißner/Leibbrand (2005) sowie Gleißner, W./Füser, K. (2014)).

8 Speziell, wenn dadurch den Unternehmen Nachteile entstehen (z. B. durch eine Self-Fulfilling-Prophecy).

9 Vgl. Risk Management Association e. V. (2019) mit einer umfassenden Darstellung.

10 Graumann, M. (2014), S. 319 und Graumann, M. et al. (2009).

koaggregation und risikogerechte Bewertung von Handlungsoptionen (zum Beispiel für eine Strategieentwicklung[11] und die Strategiebewertung). Gerade mit der Monte-Carlo-Simulation als Schlüsseltechnologie zur Aggregation von Risiken im Kontext der Unternehmensplanung werden Controlling und Risikomanagement verbunden, und es entsteht eine Bandbreitenplanung, die Scheingenauigkeiten vermeidet und Voraussetzungen schafft, um die Planungssicherheit zu verbessern und um risikoadäquat das Ertrag-Risiko-Profil von Handlungsoptionen zu vergleichen.

4. Der DIIR Revisionsstandard Nr. 2 im Überblick

Die oben erläuterten zentralen rechtlichen und ökonomischen Anforderungen an das Risikomanagement waren die Grundlage für die Entwicklung des neuen Revisionsstandards Nr. 2. Es ist der erste Prüfungsansatz, der die Vielzahl neuer Entwicklungen im Risikomanagement aufgreift und in einem Prüfungsstandard integriert, der klar auf die Erfüllung aller zentralen gesetzlichen Anforderungen – auch den Implikationen von § 93 AktG – ausgerichtet ist. Er hat in dieser Hinsicht sehr ausgeprägte Vorteile gegenüber der vorherigen Version und auch gegenüber den älteren Standards des IDW (PS 340 und PS 981), die zum Beispiel auf die Implikationen aus § 93 AktG gar nicht eingehen (und sich entsprechend nicht mit der Frage befassen, ob und inwieweit Risikoanalysen auch bei wesentlichen unternehmerischen Entscheidungen einbezogen werden).

In diesem Abschnitt wird der DIIR Revisionsstandard Nr. 2 erläutert. Das anschließende Kapitel erläutert etwas ausführlicher den zentralen Aspekt der im Standard thematisierten methodischen Prüfung, die die bisherige, primär auf Prozesse und Organisation ausgerichtete Prüfung ergänzen soll. Zentrale Aspekte der Prüfung der im Risikomanagement verwendeten Methoden sind Risikoquantifizierung und Risikoaggregation. In Kapitel sechs findet man darauf aufbauend konkrete Hilfsmittel für die Anwendung des Standards in Form von Checklisten mit den wichtigsten Prüffragen.[12]

Wesentliche Änderungen in der neuen Fassung des Revisionsstandard Nr.2 sind:

- Anpassung der Risikodefinition an Best Practice [„Möglichkeit des Eintretens von Ereignissen oder von Entwicklungen, die sich auf das Erreichen von Zielen auswirken, was die Möglichkeit von positiven Abweichungen (Chancen) und negativen Abweichungen (Gefahren, Risiken im engeren Sinn) einschließt."]
- Erweiterung der Definition von Risikomanagement:[13] „Es gehört auch zu den Aufgaben des Risikomanagements sicherzustellen, dass schon bei der Vorbereitung wesentlicher unternehmerischer Entscheidungen deren Implikationen für den zukünftigen Risikoumfang nachvollziehbar aufgezeigt werden." Das erweitert zugleich den Prüfungsauftrag.
- Ergänzung des Themas Risikokultur.
- Wichtige Klarstellung, dass die Prüfung auch die frühe Erkennung bestandsgefährdender Entwicklungen, die sich meist aus Kombinationseffekten mehrerer Einzelrisiken ergeben, umfassen muss, und dass Prüfungsgegenstand das gesamte Überwachungssystem inklusive aller Managementsysteme ist, die sich mit Risiken befassen (zum Beispiel auch des Controllings).
- Klarstellung, dass eine Prüfung der im Risikomanagement genutzten Verfahren (betriebswirtschaftlichen Methoden) im Hinblick auf die Angemessenheit zu erfolgen hat.

Der Revisionsstandard empfiehlt eine Prüfung der wichtigsten Elemente eines Risikomanagementsystems entsprechend eines Phasenmodells (siehe Abbildung 1).

Die Interne Revision hat Angemessenheit und Wirksamkeit der Maßnahmen und Kontrollen zur internen Risikosteuerung zu beurteilen.[14] Hervorzuheben ist zunächst, dass der neue DIIR Revisionsstandard Nr. 2 nun erstmals zwei große Prüfungsfelder deutlich getrennt aufzeigt:

1. Die Prüfung von Organisation und Prozessen im Risikomanagement.
2. Die Prüfung der im Risikomanagement eingesetzten betriebswirtschaftlichen Methoden (zum Beispiel zur Risikoquantifizierung und Risikoaggregation).

Ein in vielen Studien zum Risikomanagement aufgezeigtes Problem besteht bisher darin, dass die Prüfung des Risikomanagements bisher primär

11 Vgl. Schwenker, B./Dauner-Lieb, B. (2017).

12 Vgl. auch Gleißner, W./Sassen, R./Behrmann, M. (2019). Eine ausführlichere Liste von Prüffragen unter https://www.diir.de/fileadmin/downloads/arbeitskreise/20181212_Pr%C3%BCfungsleitfaden_DIIR_Standard_Nr_2_Vs_2.0.xlsx (Stand: 10.05.2019).

13 Sowie Ergänzung der Definitionen für Risikoaggregation sowie bestandsgefährdende Entwicklung.

14 Siehe DIIR Revisionsstandard Nr. 2 (2018), RZ 64.

Abb. 1: Phasenmodell des Risikomanagements

auf Organisation und Prozesse ausgerichtet war (zum Beispiel die Prozesse für Risikoanalyse, Risikoüberwachung oder Risikoreporting). Ob die hier genutzten Methoden aber überhaupt geeignet sind, um den (gesetzlichen) Zielen des Risikomanagements gerecht zu werden, wurde mit deutlich weniger Intensität betrachtet. Eine Konsequenz ist, dass in vielen Unternehmen trotz oft scheinbar ordentlichen Risikomanagementprozessen und einer sachgemäßen Organisation zugleich gravierende methodische Defizite bestehen, beispielsweise dergestalt, dass durch das Fehlen einer adäquaten Methode für die Risikoaggregation gar nicht beurteilt werden kann, ob bestandsgefährdende Entwicklungen aus Kombinationseffekten von Einzelrisiken auftreten können.

Besonders hervorzuheben sind zudem insbesondere folgende Aspekte des Standards:

1. Risiko wird verstanden als Überbegriff zu möglichen positiven Abweichungen (Chancen) und negativen Abweichungen (Gefahren, Risiken im engeren Sinn) (siehe RZ 15).
2. Mit Bezug auf die gesetzliche Anforderung aus § 91 (2) AktG im Hinblick auf die Erkennung möglicher bestandsgefährdender Entwicklungen wird die Methode zur Risikoaggregation zum zentralen Prüfungsfeld, weil nur so gewährleistet werden kann, dass auch mögliche bestandsgefährdende Entwicklungen aus Kombinationseffekten von Einzelrisiken erfasst werden (siehe RZ 19). Entsprechend heißt es in RZ 60: „Die Methode der Risikoaggregation, die gewährleistet, dass auch die Kombinationseffekte von Einzelrisiken im Hinblick auf eine sich daraus ergebende bestandsgefährdende Entwicklung erkannt werden, ist zu prüfen." Wesentlich ist, dass klarer als im alten IDW PS 340 betont wird, dass die Risikoaggregation grundsätzlich Prüfungsgegenstand sein muss. Auch der sich aus einer Risikoaggregation ergebende ökonomische Mehrwert wird klar adressiert:[15] „Die Risikoaggregation erlaubt die Berechnung von Kennzahlen für den Gesamtrisikoumfang (Value-at-Risk oder Eigenkapitalbedarf) und daraus ableitbaren Größen (wie Insolvenzwahrscheinlichkeit oder risikogerechte Kapitalkosten)."
3. Da Risikoaggregation eine Risikoquantifizierung erfordert, wird diese zum Prüffeld für die Interne Revision. Dazu liest man in RZ 58: „Die Quantifizierung von Einzelrisiken ist notwendige Voraussetzung, um mittels Risikoaggregation den Risikoumfang des betrachteten Bewertungsobjekts zu bestimmen. Der Gesamtrisikoumfang sollte durch geeignete Risikomaße ausgedrückt werden (zum Beispiel Value-at-Risk, Eigenkapitalbedarf oder Variationskoeffizient der Erträge)." Weiter heißt es in RZ 58: „Die Risikoquantifizierung ist die Beschreibung von Risiken mittels einer geeigneten Dichte- oder Verteilungsfunktion, mit historischen Daten (wie zum Beispiel einer Liste der Schadensfälle) oder einer Häufigkeitsverteilung aus einer Monte-Carlo-Simulation."
4. Der DIIR Revisionsstandard Nr. 2 betont also klar die Notwendigkeit der Quantifizierung von Risiken (ganz auf Linie des IDW PS 340) und empfiehlt die darauf aufbauende Messung der Risikotragfähigkeit (wie IDW PS 981). Hierzu führt der Standard aus (siehe RZ 21 und RZ 22): „Es empfiehlt sich, Kennzahlen zu definieren, die den Gesamtrisikoumfang in Relation bringen zum Risikodeckungspotenzial des Unternehmens." und „Beispielsweise können Kennzahlen für die Risikotragfähigkeit angegeben werden, die den Abstand des Status quo zu dem Punkt, der als bestandsgefährdende Entwicklung angesehen werden muss, und die Wahrscheinlichkeit, dass eine solche bestandsgefährdende Entwicklung auftritt, zeigen." Dazu wird in RZ 53 erläutert: „Die Risikotragfähigkeit kann oft auch über eine Abschätzung der maximalen Risikowirkung (zum Beispiel in Euro), die eine Organisation über-

15 Siehe DIIR Revisionsstandard Nr. 2 (2018), RZ 20.

stehen kann, gemessen werden." Weiter heißt es in RZ 54: „Damit wird die Risikotragfähigkeit über das wirtschaftliche Eigenkapital erfasst, das als Haftungsmasse zur Vermeidung einer Überschuldung zur Verfügung steht. Da Insolvenzen auch durch Zahlungsunfähigkeit ausgelöst werden, sind weitergehende Risikotragfähigkeitskonzepte sinnvoll."

5. Von grundlegender Bedeutung ist es, dass bei der Prüfung des Risikomanagements auch schon die Implikationen aus § 93 AktG im Hinblick auf ein entscheidungsorientiertes Risikomanagement berücksichtigt werden. Entsprechend klar wird zu den Aufgaben des Risikomanagements ausgeführt (siehe RZ 16): „Es gehört auch zu den Aufgaben des Risikomanagements sicherzustellen, dass schon bei der Vorbereitung wesentlicher unternehmerischer Entscheidungen deren Implikationen für den zukünftigen Risikoumfang nachvollziehbar aufgezeigt werden, um zumindest eine mit solchen Entscheidungen möglicherweise einhergehende bestandsgefährdende Entwicklung früh zu erkennen. Neben bereits vorhandenen Risiken, sind damit durch das Risikomanagement insbesondere auch geplante Maßnahmen und Entscheidungen zu betrachten, speziell im Hinblick auf durch diese möglicherweise verursachten zukünftigen Risiken." Ergänzend liest man in RZ 25: „Zu einer erfolgreichen und wertorientierten Führung einer Organisation im Sinne einer guten Corporate Governance gehört ein auf die Risikolage fokussierendes Überwachungssystem. Neben der Überwachung vorhandener Risiken ist das System der Vorbereitung von Managemententscheidungen einzubeziehen, um die Auswirkungen von Entscheidungen auf die Risikolage zu erfassen."
6. Anders als in früheren Standards wird klar ausgedrückt, dass die Prüfung eines Risikomanagementsystems sich sowohl auf die betriebswirtschaftlichen Methoden als auch auf Organisation und Systemaufbau zu beziehen hat. So liest man in RZ 33: „Die Prüfung der betriebswirtschaftlichen Methoden betrachtet die im Risikomanagement genutzten Verfahren im Hinblick auf die Angemessenheit zur Erfüllung der gesetzten Ziele. Geprüft werden müssen dabei insbesondere die Eignung der Methoden der Risikoidentifikation, die Eignung der genutzten quantitativen Verfahren zur Beschreibung von Risiken (Wahrscheinlichkeitsverteilung, stochastische Prozesse) und die Methoden der Risikoaggregation, speziell auch im Hinblick auf die Eignung, bestandsgefährdende Entwicklungen aus den Kombinationseffekten von Einzelrisiken zu erkennen. Ebenso zu prüfen sind die Methoden zur Berücksichtigung von Risikoinformationen bei der Entscheidungsvorbereitung."

> **In vielen Unternehmen bestehen gravierende methodische Defizite dergestalt, dass gar nicht beurteilt werden kann, ob bestandsgefährdende Entwicklungen aus Kombinationseffekten von Einzelrisiken auftreten können.**

7. Der DIIR Revisionsstandard Nr. 2 betont die Bedeutung einer Risikokultur und macht sie zum Prüfungsgegenstand. In RZ 38 liest man: „Basis für ein effektives Risikomanagementsystem ist eine Risikokultur, die einen offenen Umgang mit Risiken unterstützt."
8. Der strategische Fokus des Risikomanagements wird hervorgehoben, ähnlich wie in der neuen Version von COSO Enterprise Risk Management (ERM) von 2017. Der Fokus bei der Risikoidentifikation sind gemäß DIIR strategische Risiken (sowie unsichere Planannahmen). In RZ 45 liest man: „Besondere Beachtung finden müssen dabei die strategischen Risiken, die die wesentlichen Erfolgspotenziale bedrohen und die im Allgemeinen nur unter Einbeziehung der Geschäftsleitung analysiert werden können." In RZ 41 liest man: „Die Risikostrategie ist aus der Gesamtstrategie der Organisation abgeleitet. Sie umfasst die Risikobereitschaft der Geschäftsleitung unter Berücksichtigung des Risikodeckungspotenzials der Organisation, die Ziele der Risikosteuerung der wesentlichen Geschäftsaktivitäten sowie die Maßnahmen zur Erreichung dieser Ziele. Sie sollte so ausgestattet sein, dass die operative Steuerung der Risiken daraus abgeleitet werden kann." Hier wird (wie auch an anderen Stellen) deutlich, dass Prüfungsgegenstand ein umfassendes Risikomanagement und nicht nur das Risikofrüherkennungssystem ist, da insbesondere auch die Maßnahmen mit einbezogen werden (wie auch im IDW PS 981, nicht aber im IDW PS 340).
9. Die Einbeziehung anderer Managementsysteme, zum Beispiel des Controllings, in die Prüfung des Risikomanagements, sofern sich diese mit Risiken befassen, wird im neuen

Standard Nr. 2 klar ausgedrückt. So liest man in RZ 45 „Auch die systematische Erfassung von unsicheren Annahmen, die im Planungs- und Budgetierungsprozess, aber auch bei Entscheidungen im Kontext neuer Technologien gesetzt werden, ist eine wichtige Quelle der Risikoidentifikation." Auf die Bedeutung der in vielen Unternehmen bisher wenig beachteten Extremrisiken weist der Standard hin. In RZ 45 heißt es: „Bestandsgefährdende Entwicklungen hängen oft von solchen seltenen Extremrisiken (oder Kombinationen von Risiken) ab, weshalb deren frühzeitige Erkennung wichtig ist."

10. Der DIIR Revisionsstandard Nr. 2 betont die Aufgabenteilung zwischen Risikomanagement und operativem Management. Man liest in RZ 61: „Gemäß dem Three-Lines-of-Defense-Modell liegen Aufgaben zur Risikoüberwachung sowohl beim operativen Management (Risk Owner) als auch bei zentralen Überwachungsfunktionen (zum Beispiel Risikocontrolling oder zentrales Risikomanagement)."
11. Der DIIR Revisionsstandard Nr. 2 stellt klar, dass das wesentliche Ziel der Risikoberichterstattung und -kommunikation darin besteht, dass Entscheidungsträger und Aufsichtsorgane zeitnah über die Risikolage der Organisation informiert werden. Zu einer derartigen Information tragen auch Ad-hoc-Risikomeldungen bei (für die adäquate Schwellenwerte zu definieren sind). Entsprechend nennt der Standard in RZ 70 in diesem Bereich folgende wesentliche Prüfungsaspekte:
    - festgelegte Rahmenbedingungen der Berichterstattung,
    - Regeln für die Ad-hoc-Berichterstattung,
    - Verständlichkeit der Berichterstattung,
    - Darstellung der Ergebnisse der Risikoaggregation, um mögliche bestandsgefährdende Entwicklungen aus Kombinationseffekten von Einzelrisiken zu erkennen,
    - Berücksichtigung von Risikoinformationen bei wesentlichen unternehmerischen Entscheidungen.

Die Einhaltung der Vorgaben bei der Kommunikation soll dabei durch die Revision (mittels Stichproben) geprüft werden. (Dies bedeutet zu untersuchen, ob in Entscheidungsvorlagen eines Vorstands beziehungsweise Geschäftsführers entscheidungsvorbereitende Risikoanalysen dokumentiert sind).

5. Methodische Prüfschwerpunkte: Fähigkeit zur Erkennung bestandsgefährdender Entwicklungen, Risikoquantifizierung und Risikoaggregation

Wie oben ausgeführt, erfordert eine umfassende Prüfung des Risikomanagements durch die Interne Revision (oder einen Wirtschaftsprüfer oder spezialisierten Berater) auch eine Prüfung der im Risikomanagement genutzten betriebswirtschaftlichen Methoden, speziell auch der quantitativen Methoden (da Risiko eben ein Wahrscheinlichkeitskonzept ist). Da dieser Prüfungsschwerpunkt für die Interne Revision oft noch relativ neu ist, werden nachfolgend einige bedeutsame Grundlagen zur Risikoquantifizierung und Risikoaggregation knapp skizziert.

Gefordert wird im DIIR Revisionsstandard Nr. 2 (wie auch im IDW PS 340 und IDW PS 981) die Aggregation aller (wesentlichen) Risiken über alle Risikoarten und auch über die Zeit. Da nur quantifizierte Risiken auch aggregiert werden können, ist das Gebot der Quantifizierung sämtlicher Risiken nur konsequent.

Die Quantifizierung von Risiken erfordert die Zuordnung geeigneter Wahrscheinlichkeitsverteilungen (oder stochastischer Prozesse) unter Nutzung der besten verfügbaren Informationen, die durchaus auch subjektive Expertenschätzungen sein können.[16] Bekanntlich ist es in vielen Fällen insbesondere nicht sachgerecht, wenn ein Risiko nur durch Eintrittswahrscheinlichkeit und Schadenshöhe beschrieben wird. Selbst bei sogenannten ereignisorientierten Risiken[17] ist die Auswirkung unsicher und damit ist es notwendig, die Auswirkungen durch eine Bandbreite zu beschreiben (also zum Beispiel durch die Angabe von Mindestwert, wahrscheinlichstem Wert und Maximalwert eines möglichen Schadens). Die Prüfung der Angemessenheit der quantitativen Beschreibung eines Risikos ist ein wesentliches Thema für die methodische Prüfung des Risikomanagements.[18]

Durch die Aggregation im Kontext der Planung – Chancen und Gefahren verstanden als Ursache möglicher Planabweichungen – muss untersucht werden, welche Auswirkungen diese

16 Siehe dazu Gleißner, W. (2017a) und Sinn, H.W. (1980) zu den Grundlagen zur subjektiven Schätzung von Wahrscheinlichkeiten und der Möglichkeit einer Überführung von Unsicherheit in (quantifiziertes) Risiko.
17 Füser, K./Gleißner, W./Meier, G. (1999).
18 Siehe die Checkliste für derartige Prüfungen bei Gleißner, W. (2019a) sowie Gleißner, W./Wolfrum, M. (2015) zum Umgang mit Datenproblemen bei der Risikoquantifizierung.

auf den zukünftigen Ertrag, die wesentlichen Finanzkennzahlen, Kreditvereinbarungen (Covenants) und das Rating haben. So ist beispielsweise zu untersuchen, mit welcher Wahrscheinlichkeit durch den Eintritt bestehender Risiken (zum Beispiel Konjunktureinbruch in Verbindung mit einem gescheiterten Investitionsprojekt) das durch Finanzkennzahlen abschätzbare zukünftige Rating des Unternehmens unter ein für die Kapitaldienstfähigkeit notwendiges Niveau (B-Rating) abfallen könnte. Gerade die aus der Risikoaggregation ableitbaren Ratingprognosen verknüpfen Unternehmensplanung und Risikoanalyse und stellen so den wichtigsten Krisenfrühwarnindikator dar. Ohne diese gemeinsame Betrachtung, also die Risikoaggregation, ist eine mögliche Bestandsbedrohung des Unternehmens nicht erkennbar.

Beispiel: Der Vorstand entscheidet sich mit Zustimmung des Aufsichtsrats für eine Großinvestition, bei der keine bestandsbedrohenden Einzelrisiken gesehen werden. Diese Beurteilung der Risikolage ist korrekt. Dennoch entstehen später Schäden durch eine existenzbedrohende Krise, weil zwei Risiken, Großkundenverlust und Scheitern des Investitionsprojekts, gemeinsam eingetreten sind. Hätte man die Kombinationseffekte und ihre Implikationen für das Rating vor der Entscheidung ausgewertet, hätte man die Bedrohung erkannt und im Rahmen der Entscheidungsfindung gewürdigt (und das Projekt zum Beispiel verschoben, das Eigenkapitel erhöht etc).

Die Aggregation von Risiken im Kontext der Unternehmensplanung erfordert zwingend den Einsatz von Simulationsverfahren (Monte-Carlo-Simulation), weil Risiken nicht addierbar sind. Mittels Computersimulation wird bei der Risikoaggregation eine große repräsentative Anzahl risikobedingt möglicher Zukunftsszenarien (Planungsszenarien) analysiert. Auf diese Weise wird eine realistische Bandbreite der zukünftigen Erträge und Liquiditätsentwicklung aufgezeigt, also die Planungssicherheit beziehungsweise der Umfang möglicher negativer Planabweichungen dargestellt (siehe auch Abbildung 2). Unmittelbar ableiten kann man die Wahrscheinlichkeit, dass Covenants verletzt werden oder ein Zielrating nicht mehr erreicht wird. Auch die weiterführende Ableitung risikogerechter Kapitalkostensätze als Anforderung an die Rendite einzelner Projekte und Geschäftsfelder ist möglich, ohne dass man auf historische Kapitalmarktdaten zurückgreifen müsste.

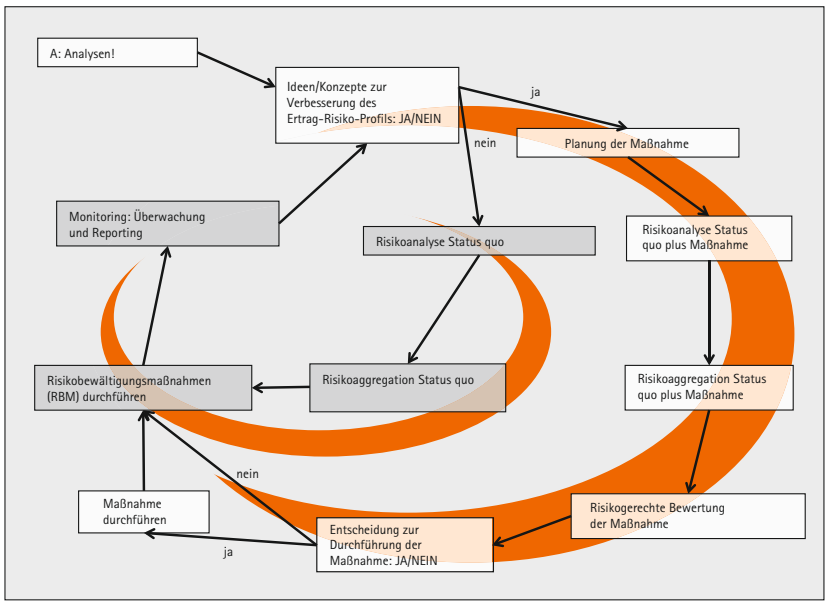

Abb. 2: Risikoanalyse und Bewertung zur Entscheidungsvorbereitung[19]

In manchen Unternehmen wird versucht, statt einer echten, simulationsbasierten Risikoaggregation, ausgehend von Risikoinventar oder Risk-Map, die Ergebnisauswirkungen wichtiger Risiken in zwei oder drei Einzelszenarien, inklusive eines Worst-Case-Szenarios, abzuschätzen. Dieses Vorgehen ist nahezu nutzlos, es ist willkürlich konstruiert und die Wahrscheinlichkeit, dass dieses oder ein schlimmeres Szenario eintritt, unbestimmt. Ein echtes Worst-Case-Szenario ist wenig hilfreich: Im Worst Case, bei Eintreten sämtlicher Risiken, ist jedes Unternehmen insolvent. Ob die betrachteten zwei oder drei von unendlich vielen risikobedingt möglichen Zukunftsszenarien tatsächlich in irgendeiner Weise hilfreich sind, muss bezweifelt werden. Bei einer Monte-Carlo-Simulation als Risikoaggregationsverfahren werden zum Beispiel repräsentativ ausgewählte 100.000 Szenarien betrachtet und auf dieser Grundlage wird abgeleitet, welcher Anteil dieser Szenarien bestandsbedrohend ist. Man gibt also nicht weitgehend willkürlich Szenarien vor, sondern analysiert Häufigkeit und Charakteristika der kritischen Szenarien. So kann man beispielsweise herausfinden, welche Kombinationen von Risiken (mit welcher Ausprägung) für das Unternehmen und sein Rating problematisch sind, um geeignete Risikobewältigungsmaßnahmen zu initiieren oder die Strategie robuster zu gestalten. Abbildung 3 zeigt, wie durch die Kombination von Planung und Risikoanalyse mittels Risikoaggregation die relative Häufigkeit von Insolvenzszenarien berechnet und als Ratingnote ausgedrückt werden kann.

19 Siehe Quelle: Gleißner, W. (2015) und (2018a).

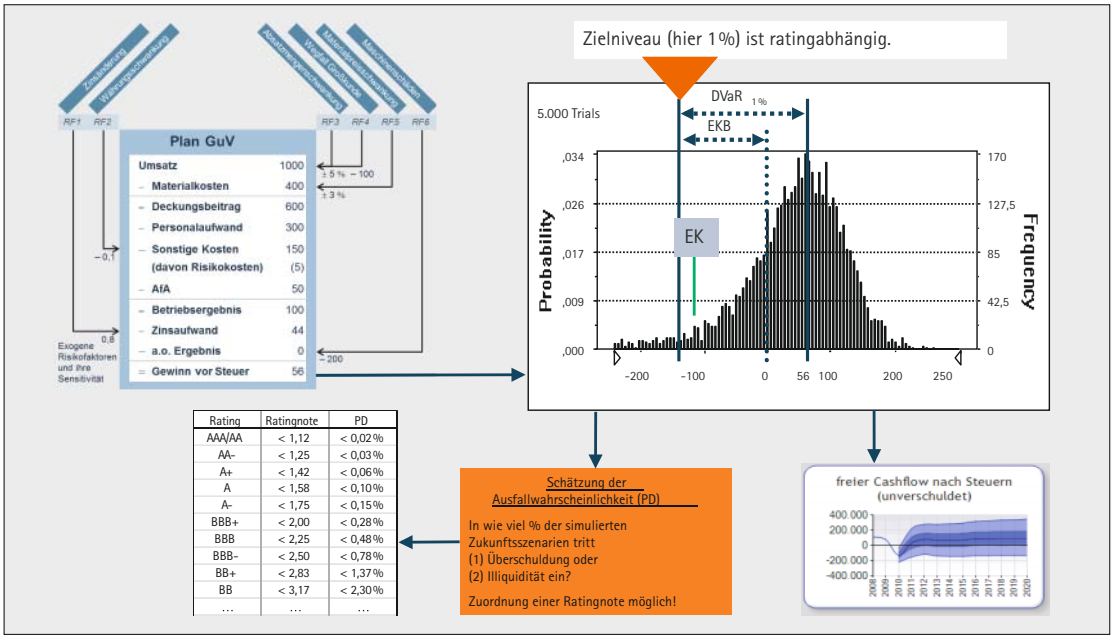

Abb. 3: Risikoanalyse und Risikosimulation (inklusive Ratingprognose)

Aufbauend auf der nötigen Risikoaggregation empfiehlt der Standard Nr. 2 wie auch der IDW PS 981 zur Prüfung des Risikomanagements die Einführung eines Risikotragfähigkeitskonzepts, das den Abstand zur bestandgefährdenden Entwicklung misst. Risikotragfähigkeit korrespondiert dabei unmittelbar mit der gesetzlichen Anforderung bestandsgefährdende Entwicklungen früh zu erkennen (§ 91 AktG). Die Risikotragfähigkeit drückt entsprechend, den Abstand zwischen der aktuellen Situation und dem Punkt aus, bei dem man von einer Bestandsgefährdung ausgehen muss (in Euro oder alternativ auch zum Beispiel in Prozent des EBITDA).

Von einer bestandsgefährdenden Entwicklung ist im Allgemeinen auszugehen,

1. wenn das Eigenkapital verzehrt wird (Überschuldung) oder
2. bei einer drohenden Illiquidität, weil
   a. Kreditvereinbarungen (Covenants) verletzt werden, die eine Kündigung der Kredite zur Folge haben, oder
   b. für die Finanzierung erforderliche Mindestanforderungen an das Rating nicht mehr gewährleistet sind (zum Beispiel Unterschreiten eines B-Ratings).

Viele Unternehmen hoher Bonität haben einen so hohen Abstand zu dem kritischen Punkt der Bestandsgefährdung, dass diese für die Unternehmenssteuerung ergänzend einen zweiten Schwellenwert betrachten, bezüglich dem die Risikotoleranz gemessen wird. Für manche Unternehmen bester Bonität ist diese Schwelle zum Beispiel der Investmentgrade BBB-. Untersucht wird, welche negativen EBIT-Auswirkungen durch Risiken maximal zu verkraften wären, bevor der Investmentgrade verloren geht.[21] Für ein typisches mittelständisches Unternehmen mag dagegen die Risikotoleranz in Bezug auf die Schwelle des BB-Rating geschätzt werden.

Für die Quantifizierung der Risikotragfähigkeit benötigt man geeignete Kennzahlen.[22] So kann man die Risikotragfähigkeit beispielsweise messen durch

a) den maximal möglichen Verlust, den ein Unternehmen verkraften kann, bis eine bestandsgefährdende Entwicklung eintritt (zum Beispiel durch die Verletzung von Mindestanforderungen an das Rating) und
b) die Wahrscheinlichkeit dafür, dass es durch Kombinationseffekte von Einzelrisiken zu einer solchen bestandsgefährdenden Entwicklung kommt (was sich unmittelbar aus der Risikoaggregation ableiten lässt).

6. Prüfung der Angemessenheit und Wirksamkeit des Risikomanagements

5.1 Grundlagen

Es existieren verschiedene sich ergänzende Strategien für eine schnelle und effiziente Prüfung des Risikomanagements.[23]

1. Die Systemprüfung, die Anforderungen an das Risikomanagementsystem prüft,

20 Vgl. Gleißner, W. (2017a), S. 413.

21 Siehe dazu auch Gleißner, W. et al. (2011).

22 Für die Risikotoleranz bezogen auf das anspruchsvollere Sicherheitsziel gilt dies analog.

23 Vgl. Gleißner, W. (2017c).

lfd. Nr.	Prüfungsfeld	Thema	Frage	Prüfungshinweise
1.1.3	Organisation und Risikokultur	Vorgaben	Hat die Geschäftsleitung die Rahmenbedingungen und Ziele für die Organisation des Risikomanagements definiert?	Definition von Rollen, Eskalationsmechanismen, Prozesse, Informationswege, regelmäßige und Ad-hoc-Berichterstattung, Kommunikation
2.1.2	Strategie	Risikostrategie allgemein	Wurde die Risikostrategie von der Geschäftsleitung diskutiert und kommuniziert?	Gibt es eine nachvollziehbare Dokumentation der Entscheidung und der Grundannahmen auf der diese Risikostrategie basiert? Werden Änderungen in den Annahmen der Risikostrategie dem Management bekannt gemacht und reagiert das Management auf diese Information angemessen?
3.3.3	Identifikation und Erfassung	Vollständigkeit	Werden alle relevanten Geschäftsbereiche und Organisationseinheiten in die Risikoidentifikation einbezogen?	Vorgabe eines festen Rasters zur Einordnung und Systematisierung von Risiken, Risikofeldern und Risikobereichen (inkl. Projekte) nach internen/externen Risiken, nach Funktionsbereichen, nach direkten/indirekten Effekten (Reputationsrisiken) inklusive Top-down-Ansatz mit strategischen Risiken ...
4.3.1	Analyse und Bewertung	Auswirkungen	Werden für sämtliche Risiken die Auswirkungen ermittelt?	Die im Risikoinventar erfassten Risiken sind im Rahmen der Risikoanalyse hinsichtlich der Ursache-Wirkungs-Zusammenhänge zu untersuchen sowie im Hinblick auf ihre quantitativen Auswirkungen und ihre Eintrittswahrscheinlichkeit einzuschätzen ...
5.2.1	Steuerung und Überwachung	Kontrollaktivitäten	Sind Kontrollaktivitäten für die einzelnen Risikosteuerungsmaß-nahmen benannt worden (Vollständigkeit), die eine wirksame Umsetzung der Risikosteuerungsmaßnahmen sicherstellen (Eignung)?	Kontrollaktivitäten stellen sicher, dass Risikosteuerungsmaßnahmen angemessen (in korrekter Weise und zeitnah) ausgeführt werden.
6.1.1	Risikoberichterstattung	Risikoberichterstattung (Grundlagen)	Ist prozessual sichergestellt, dass die Geschäftsleitung regelmäßig über die Themen mit Risikobezügen diskutiert?	Regelmäßige Vorlage des Risikoberichts und Befassung in der Geschäftsleitung, regelmäßiger Jour fixes mit der Geschäftsleitung, Reporting an die Geschäftsleitung.

Tab. 1: Auszüge aus der DIIR-Checkliste

2. Die Outputprüfung, die hinterfragt, ob vom Vorstand diejenigen Informationen dem Aufsichtsrat angeboten werden, die ein Risikomanagementsystem liefern sollte,
3. Die Abweichungsanalyse, die überprüft, ob eingetretene Planabweichungen auf im Vorhinein bekannte Risiken zurückgeführt werden können.

Die Interne Revision wird einen großen Teil ihrer Zeit für die Systemprüfung des Risikomanagementsystems einsetzen, die daher nachfolgend im Mittelpunkt steht. Der DIIR Revisionsstandard Nr. 2 ist wie oben erläutert mehr als eine Grundlage für eine formale Systemprüfung. Es gilt insgesamt die Angemessenheit und Wirksamkeit zu prüfen (vgl. RZ 31).

5.2 Prüfkriterien des DIIR Revisionsstandard Nr. 2: Eine Checkliste

Der Revisionsstandard Nr. 2 bietet, wie oben erläutert, eine sehr gute Grundlage für eine umfassende Prüfung des Risikomanagements mit der Zielsetzung, Lücken und vor allen Dingen auch Verbesserungspotenziale aufzuzeigen. Der gemeinsame Arbeitskreis von DIIR und RMA hat für die Unterstützung der Prüfungsaktivitäten ergänzend eine Liste von Prüfkriterien (als Leitfaden) erstellt.[24] Tabelle 1 enthält auszugsweise Fragen der Checkliste mit ergänzenden Prüfungshinweisen, jeweils eine aus den jeweiligen Phasen des Risikomanagements.

Die Checkliste beinhaltet ein Bewertungssystem, bei den Hauptfragen mit einem Wert von null (nicht erfüllt), eins (schlecht erfüllt), zwei (teilweise erfüllt) oder drei (voll erfüllt) bewertet werden. Werden mehr als 70 Prozent der maximal zu vergebenden Punkte erreicht, so kann ein insgesamt positives Urteil zur Wirksamkeit des Risikomanagementsystems unterstützt werden, solange die definierten 22 Mindestanforderungen erfüllt sind. Bei Erreichen von weniger als 50 Prozent der Punkte, sollte nicht mehr von einem insgesamt wirksamen System gesprochen werden. Die Ergebnisse können mithilfe vordefi-

24 Verfügbar unter https://www.diir.de/fileadmin/downloads/arbeitskreise/20181212_Pr%C3%BCfungsleitfaden_DIIR_Standard_Nr_2_Vs_2.0.xlsx (Stand: 10.05.2019).

nierter Balken- oder Netzdiagramme visualisiert werden. Die Excel-Checkliste bietet dem Revisor eine gute Grundlage für eine angemessene Prüfungsdurchführung und Berichterstattung. Sie dient gleichzeitig der unternehmensübergreifenden Standardisierung der Prüfung von Risikomanagementsystemen.

7. Fazit

Sowohl Anforderungen[25] als auch Status des Risikomanagements in deutschen Unternehmen haben sich in den letzten 20 Jahren seit Inkrafttreten des KonTraG deutlich verändert. Diesen Veränderungen wird der neue DIIR Revisionsstandard Nr. 2 gerecht. Gegenstand des Risikomanagements sind heute sowohl mögliche positive wie negative Planabweichungen (Chancen und Gefahren), wie es zum Beispiel auch COSO ERM, ISO 9001, ISO 31000 und IDW PS 981 betonen. Weiterhin ist es die gesetzliche Mindestanforderung, mögliche bestandsgefährdende Entwicklungen – auch aus Kombinationseffekten mehrerer Einzelrisiken – früh zu erkennen. Die Risikoaggregationsmodelle sollten um Verfahren zur Messung von Risikotragfähigkeit und Risikotoleranz ergänzt werden (siehe DIIR Revisionsstandard Nr. 2 und IDW PS 981). Während ursprünglich primär die Möglichkeit einer Überschuldung betrachtet wurde, muss heute ergänzend die Möglichkeit einer drohenden Illiquidität durch die Verletzung von Covenants oder Mindestanforderungen an das Rating betrachtet werden. Die Insolvenzwahrscheinlichkeit kann als Messgröße für das Insolvenzrisiko und den Grad der Bestandsgefährdung eines Unternehmens als die Spitzenkennzahl des Risikomanagements aufgefasst werden und ist zugleich ein wichtiger Werttreiber.

Als die wichtigste Veränderung des Risikomanagements ergibt sich die in der Zwischenzeit auch gebotene entscheidungsorientierte Ausrichtung, die man seit 2017 auch im neuen COSO Enterprise Risk Management Framework findet. Um die gemäß § 93 AktG geforderten angemessenen Informationen bei der Vorbereitung unternehmerischer Entscheidungen des Vorstands aufweisen zu können, ist nämlich insbesondere eine Risikoanalyse notwendig, die aufzeigt, welche Veränderung des Risikoumfangs sich durch eine Entscheidung ergeben würde. Zudem sollte Risikomanagement als Querschnittsfunktion verstanden werden, die in andere Managementsysteme integriert ist (wie Controlling und Qualitätsmanagement). Eine klarere Fokussierung der Prüftätigkeit der Internen Revision auf diese zentralen Fragestellungen ist empfehlenswert.

Der neue Revisionsstandard Nr. 2 ist ein Prüfungsstandard für das Risikomanagement, der alle wesentlichen Aspekte und Themen aufgreift. Neue Anforderungen an das Risikomanagement (zum Beispiel infolge § 93 AktG mit seinen Implikationen für entscheidungsvorbereitende Risikoanalyse) werden ebenso betrachtet wie schon länger bekannte Anforderungen (insbesondere aus § 91 (2) AktG/KonTraG). Das gesamte Spektrum relevanter Anforderungen an ein Risikomanagementsystem – von Risikokultur über die Methoden zur Risikoquantifizierung und Risikoaggregation bis hin zu Angemessenheit und Wirksamkeit von Prozessen und Maßnahmen – werden betrachtet. Es ist besonders positiv hervorzuheben, dass nunmehr die gesetzlichen Kernanforderungen an ein Risikomanagement aus § 91 AktG – frühe Erkennung möglicher bestandsgefährdender Entwicklungen – in besonderer Weise beachtet wird (zum Beispiel durch die klare Verpflichtung, die Risikoaggregationsmodelle zu prüfen, die erforderlich sind, bestandsgefährdende Entwicklungen aus Kombinationseffekten von Einzelrisiken zu erfassen).

Prüfungen des Risikomanagements anhand der Anforderungen aus dem DIIR Revisionsstandard Nr. 2 können zudem sehr konkrete Anregungen geben, wie ein modernes Risikomanagement entscheidungsorientiert ausgerichtet werden kann, um auch den Anforderungen aus § 93 AktG (Business Judgement Rule) gerecht zu werden. Erst ein solches Risikomanagement schafft durch seinen Beitrag zur Verbesserung unternehmerischer Entscheidungen (Berücksichtigung von Risiken im Entscheidungskalkül) ökonomischen Mehrwert.

Die Anwendung des Standards in der Prüfung des Risikomanagements durch die Interne Revision kann damit wesentlich dazu beitragen, die Leistungsfähigkeit der heute in vielen Unternehmen noch stark verbesserungswürdigen Risikomanagementsysteme tatsächlich zu verbessern und insgesamt den Stellenwert des Risikomanagements zu fördern. Die den Standard begleitende Excel-Checkliste bietet dem Revisor eine gute Hilfestellung bei der Urteilsfindung und trägt zur Standardisierung der Prüfung von Risikomanagementsystemen bei.

25 In Anlehnung an Gleißner, W. (2018a).

Literaturverzeichnis

Berger, T./Gleißner, W. (2007): Risikosituation und Stand des Risikomanagements aus Sicht der Geschäftsberichterstattung, ZCG, 2/2007, S. 62 – 68.

Blum, U./Gleißner, W./Leibbrand, F. (2005): Stochastische Unternehmensmodelle als Kern innovativer Ratingsysteme, in: IWH-Diskussionspapiere, Nr. 6, November 2005, https://www.econstor.eu/bitstream/10419/23745/1/6-05.pdf (Stand: 22.01.19).

DIIR (2018): DIIR Revisionsstandard Nr. 2: Prüfung des Risikomanagementsystems durch die Interne Revision, Version 2.0, https://www.diir.de/fileadmin/fachwissen/standards/downloads/DIIR_Revisionsstandard_Nr._2_Version_2.0.pdf (Stand: 22.01.19).

Füser, K./Gleißner, W./Meier, G. (1999): Risikomanagement (KonTraG) – Erfahrungen aus der Praxis, Der Betrieb, 15/1999, S. 753 – 758.

Gleißner, W. (2015): Controlling und Risikoanalyse bei der Vorbereitung von Top-Management-Entscheidungen – Von der Optimierung der Risikobewältigungsmaßnahmen zur Beurteilung des Ertrag-Risiko-Profils aller Maßnahmen, Controller Magazin, 4/2015, S. 4 – 12.

Gleißner, W. (2017a): Grundlagen des Risikomanagements, 3. Auflage, Verlag Vahlen, München 2017.

Gleißner, W. (2017b): Risikomanagement, KonTraG und IDW PS 340, in WPg, 3/2017, S. 158 – 164.

Gleißner, W. (2017c): Entscheidungsvorlagen für den Aufsichtsrat: Fallbeispiel Akquisition, Der Aufsichtsrat, 04/2017, S. 54 – 56.

Gleißner, W. (2017e): Was ist eine „bestandsgefährdende Entwicklung" i. S. des § 91 (2) AktG (KonTraG)?, Der Betrieb, 47/2017, 24.11.17, S. 2749 – 2754.

Gleißner, W. (2018a): Risikomanagement 20 Jahre nach KonTraG: Auf dem Weg zum entscheidungsorientierten Risikomanagement, Der Betrieb, 46/2018, 16.11.2018, S. 2769 – 2774.

Gleißner, W. (2019a): Risikoanalyse: Grundlagen der Risikoquantifizierung (Teil 1), Controller Magazin, 2/2019, S. 42 – 46.

Gleißner, W. (2019b): Risikoanalyse: Ein strukturierter Leitfaden zur Risikoquantifizierung (Teil 2), Controller Magazin, 3/2019, S. 31 – 35.

Gleißner, W./Füser (2014): Praxishandbuch Rating und Finanzierung – Strategien für den Mittelstand, 3. Auflage mit CD-ROM, Verlag Franz Vahlen, München 2014.

Gleißner, W./Sassen, R./Behrmann, M. (2019): Prüfung und Weiterentwicklung von Risikomanagementsystemen, Springer Essentials, 2019 (erscheint in Kürze).

Gleißner, W./Wolfrum, M. (2015): Problemfelder der Risikoquantifizierung, Datenprobleme und Lösungsstrategien, in: Gleißner, W./Romeike, F. (Hrsg): Praxishandbuch Risikomanagement, Erich Schmidt Verlag, Berlin 2015, S. 274 – 263.

Gleißner, W./Wolfrum, M. (2017): Risikotragfähigkeit, Risikotoleranz, Risikoappetit und Risikodeckungspotenzial, Controller Magazin, 6/2017, S. 77 – 84.

Gleißner, W./Leibbrand, F./Kamarás, E./Helm, R./Gerking, H. (2011): Krisenprävention: Stresstests für das Unternehmen? Schwächen von Stresstests, Risiko Manager, 18/2011, S. 1, 6 – 15.

Graumann, M. (2014): Die angemessene Informationsgrundlage bei Entscheidung, WISU, 3/2014, S. 317 – 320.

Graumann, M/Linderhaus, H./Grundei, J. (2009): Wann ist die Risikobereitschaft bei unternehmerischen Entscheidungen „in unzulässiger Weise überspannt"?, BFuP, 5/2009, S.492 – 505.

Link, M./Scheffler, R./Oehlmann, D. (2018): Quo vadis Risikomanagement?, Controller Magazin, 1/2018, S. 72 – 78.

Risk Management Association e. V. (Hrsg.) (2019): Managemententscheidungen unter Risiko, erarbeitet von Gleißner, W./Kimpel, R./Kühne, M./Lienhard, F./Nickert, A.-G./Nickert, C., Erich Schmidt Verlag Berlin 2019 (erscheint in Kürze).

Schwenker, B./Dauner-Lieb, B. (2017): Gute Strategie – Der Ungewissheit offensiv begegnen, Campus Verlag, Frankfurt 2017.

Sinn, H. W. (1980): Ökonomische Entscheidungen bei Ungewissheit, J. C. B. Mohr (Paul Siebeck), Tübingen 1980.

Ulrich, P. (2018): Integration von Risikoaspekten in operative Planung und Budgetierung: Was unterscheidet mittelständische Familienunternehmen von anderen Unternehmen?, ZfKE, Bd. 66 (2018), Heft 1, S. 13 – 33.