Veröffentlicht in

Der Aufsichtsrat

Heft 4/2020

Gleißner, W. / Romeike, F. (2020):

„Entscheidungsorientiertes Risikomanagement nach DIIR RS Nr. 2“,

S. 55 – 57

»AR1329714

Entscheidungsorientiertes Risikomanagement nach DIIR RS Nr. 2

Prof. Dr. Werner Gleißner/Frank Romeike

Aus den Präzisierungen zur Business Judgement Rule (§ 93AktG) ergibt sich der Bedarf für eine Neuausrichtung des Risikomanagements hin zu einem bei der Vorbereitung „unternehmerischer Entscheidungen" unterstützenden Ansatz. Dieser wird im neuen Risikomanagement-Standard des Deutschen Instituts für Interne Revision (DIIR RS 2) vom November 2018 erstmalig abgebildet und in diesem Beitrag erläutert.

I. Überblick

Der Aufsichtsrat muss sich intensiv mit dem Risikomanagement seines Unternehmens befassen und sich von der Wirksamkeit des Systems überzeugen. Da der Aufsichtsrat basierend auf §111 AktG den Vorstand überwachen muss, ist das Risikomanagement- und Überwachungssystem Teil seiner Überwachungsaufgabe.

Basierend auf § 107 Abs. 3 AktG sollte der Aufsichtsrat einen Prüfungsausschuss bestellen, der sich mit der Überwachung des Risikomanagementsystems befasst. Wird ein solcher Prüfungsausschuss nicht eingerichtet, geht der Überwachungsauftrag auf den gesamten Aufsichtsrat über. Hieraus resultieren die folgenden Aufgaben:

1. Zunächst muss der Aufsichtsrat prüfen, ob der Vorstand das nach § 91 Abs.2 AktG geforderte Risikomanagementsystem eingerichtet hat.
2. Außerdem muss seitens des Aufsichtsrats geprüft werden, ob das vom Vorstand eingerichtete Risikomanagementsystem funktionsfähig und wirksam ist.
3. Desweitern ist zu überwachen, inwieweit vom Vorstand erforderliche Maßnahmen zur Verbesserung dieser Systeme vorgenommen wurden.
4. Der Aufsichtsrat hat zu überwachen, dass die Wirtschaftlichkeit und Zweckmäßigkeit des Risikomanagementsystems gegeben sind.
5. Abschließend muss der Aufsichtsrat sich vergewissern, dass der Vorstand adäquat auf mögliche „bestandsgefährdende Entwicklungen" (§ 91 AktG) reagiert hat. Dies bedingt vor allem ein System, dass solche bestandsgefährdenden Risiken wirksam erkennen kann; auch solche aus Kombinationseffekten von Einzelrisiken.

Durch Präzisierungen bei den gesetzlichen und regulatorischen Rahmenbedingungen haben sich gerade in den letzten zwei Jahren wesentliche neue Anforderungen an das Risikomanagement ergeben, die nun erstmalig in einem Standard zusammengefasst wurden: Der DIIR Revisionsstandard Nr. 2: Prüfung des Risikomanagementsystems durch die Interne Revision (DIIR RS Nr. 2), veröffentlicht vom Institut für Interne Revision im November 2018. Der vorliegende Beitrag erläutert knapp diese Entwicklungen und erläutert die wesentlichen Neuerungen im DIIR RS Nr. 2 und den dort skizzierten Weg zu einem „entscheidungsorientierten Risikomanagement", das hilft, den Anforderungen aus der Business Judgement Rule (§ 93 AktG) bei der Vorbereitung „unternehmerischer Entscheidungen" gerecht zu werden. Der Aufsichtsrat kann bei einer Prüfung des Risikomanagements basierend auf dem neuen DIIR RS Nr. 2 ein wesentlich präziseres Bild der Leistungsfähigkeit des Risikomanagements seines Unternehmens erhalten, als dies bei einer Prüfung bisher der Fall ist (z.B. basierend auf den Prüfungsstandards IDW PS 340 und IDW PS 981).

II. Rechtliche Anforderungen und die Entwicklung im regulatorischen Umfeld

Seit Inkrafttreten des Kontroll- und Transparenzgesetzes (KonTraG) 1998 ist es die primäre Aufgabe des Risikomanagements mögliche „bestandsgefährdende Entwicklungen" (§ 91 AktG) früh zu erkennen. Neben bestandsgefährdenden Einzelrisiken sind dabei insbesondere Kombinationseffekte von Einzelrisiken zu untersuchen, die in der Regel Krisen oder gar Insolvenzen auslösen können, was eine quantitative Risikoanalyse sowie Risikoaggregation mittels stochastischer Simulation (Monte-Carlo-Simulation) erfordert.

Die wesentlichen Anforderungen an ein Risikofrüherkennungssystem fasst auch schon seit dem Jahr 1998 der IDW Prüfungsstandard 340 des Instituts der Wirtschaftsprüfer (IDW) zusammen, der auch auf die zentrale Bedeutung einer Risikoquantifizierung und Risikoaggregation verweist. Die Bedeutung der Risikoaggregation wird auch im seit September 2019 vorliegenden Entwurf für die Überarbeitung des IDW PS 340 noch stärker betont. Mit dem IDW PS 981 für die freiwillige Prüfung von Risikomanagementsystemen gibt es zudem seit 2017 einen ergänzenden Standard, der sich auch mit Risikobewältigung befasst und vor allem die zentrale Bedeutung von Konzepten für die Messung von Risikotragfähigkeit, Risikotoleranz und Risikoappetit aufzeigt.

Diese Regelwerke haben allerdings eine zentrale Anforderung an das Risikomanagement noch gar nicht thematisiert: Die

notwendige entscheidungsorientierte Ausrichtung von Risikomanagementsystemen. Gemeint ist damit ein neues Paradigma des Risikomanagements, demzufolge das Risikomanagement dazu beitragen soll, bei der Vorbereitung unternehmerischer Entscheidungen die dafür notwendigen Risiko-Informationen zu liefern. Speziell sollte durch eine Risikoanalyse aufgezeigt werden, wie sich der Umfang an Chancen und Gefahren (Risiken) infolge einer Entscheidung verändern würde. Dieses neue Paradigma eines „entscheidungsorientierten Risikomanagements" findet man vor allem in der neuen Version von COSO Enterprise Risk Management (ERM) aus dem Jahr 2017. Der ökonomische Mehrwert dieser Neuausrichtung von Risikomanagementsystemen ist offensichtlich. Das Risikomanagement soll dazu beitragen, dass schon vor einer Entscheidung deren Auswirkung auf Ertrag und Risiko gegeneinander abgewogen werden (also Handlungsoptionen risikogerecht bewertet werden). Dies geht einher mit einer engeren Verknüpfung von Risikomanagement und Controlling sowie einer engen Verzahnung des Risikomanagements mit der Unternehmensstrategie.

» Die Business Judgement Rule fordert ein entscheidungsorientiertes Risikomanagement. «

Zu beachten ist, dass diese ökonomisch wünschenswerte Neuausrichtung des Risikomanagements auch geboten ist, um die in der Zwischenzeit durch die Rechtsprechung präzisierten Anforderungen an die Vorbereitung „unternehmerischer Entscheidungen" durch Geschäftsführer und Vorstände gerecht zu werden. Gemäß der sogenannten Business Judgement Rule (BJR) in § 93 AktG muss ein Geschäftsleiter nämlich bei der Vorbereitung „unternehmerischer Entscheidungen", z.B. bezüglich einer Investition, Akquisition oder Strategie-Veränderung, nämlich beweisbar „angemessene Informationen" vorliegen haben (eine analoge Anforderung gilt für GmbH-Geschäftsführer). Da die Auswirkungen unternehmerischer Entscheidungen unsicher sind, sind es insbesondere die Ergebnisse einer entscheidungsvorbereitenden Risikoanalyse, die in einer Entscheidungsvorlage zu dokumentieren sind.

Besonders wesentlich ist, dass die zentrale Anforderung aus § 93 AktG, demzufolge ein Vorstand bei einer „unternehmerischen Entscheidung" belegbar angemessene Informationen vorliegen haben muss, auch dann bestehen bleibt, wenn bei einem zustimmungspflichtigen Geschäft der Aufsichtsrat zustimmt. Bei Umsetzung der skizzierten Anforderungen durch den Vorstand kann ein Aufsichtsrat erwarten, dass er bei zustimmungspflichtigen Geschäften oft deutlich bessere Entscheidungsvorlagen erhält. Insbesondere muss in einer neutralen Entscheidungsvorlage über die bestehende Handlungsoption, zugrundeliegende Annahmen und speziell die mit der Entscheidung verbundenen Chancen und Gefahren (Risiken) informiert werden. Zu beachten ist, dass der Vorstand nicht die Verantwortung übernehmen kann – und damit nicht haftet – wenn die mit unternehmerischen Entscheidungen unvermeidlich verbundenen Risiken sich tatsächlich einmal realisieren. Problematisch ist es jedoch, wenn nach einer unternehmerischen Entscheidung (z.B. bezüglich einer Investition oder Akquisition) Planabweichungen eintreten, die nicht auf in der Entscheidungsvorlage genannte Risiken zurückzuführen sind oder wenn diese in einem Umfang auftreten, der durch die entscheidungsvorbereitende Risikoanalyse nicht erklärt werden kann. Dies kann als Indiz dafür gesehen werden, dass die Entscheidungsvorlage grundlegende Schwächen aufgewiesen hat und möglicherweise eine Sorgfaltspflichtverletzung des Vorstands vorliegt, die der Aufsichtsrat – gestützt auf die der „unternehmerischen Entscheidung" zugrundeliegenden Entscheidungsvorlage – zu untersuchen hat.

III. Der DIIR RS Nr. 2: ein nützlicher Standard für das Risikomanagement

Mit dem DIIR Revisionsstandard Nr. 2 des Instituts für Interne Revision e.V. (vom November 2018) liegt erstmalig ein Risikomanagement-Standard vor, der die Anforderungen aus § 91 und § 93 AktG gemeinsam betrachtet. Er ist klar fokussiert auf die Erfüllung der gesetzlichen Kernanforderungen (wie die frühe Identifikation möglicher „bestandsgefährdender Entwicklungen" im Sinne des § 91 AktG).

Die Anwendung des DIIR Revisionsstandard Nr. 2 durch die Interne Revision (oder Berater oder auch Wirtschaftsprüfer, denen ein vergleichbarer Standard noch fehlt) kann dazu beitragen, bestehende Lücken im Risikomanagement aufzudecken und diese zu schließen. Hervorzuheben ist, 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 (z. B. zur Risikoquantifizierung und Risikoaggregation).

Ein in vielen Studien zum Risikomanagement aufgezeigtes Problem besteht bisher darin, dass die Prüfung des Risikomanagements primär auf Organisation und Prozesse ausgerichtet war (z. B. die Prozesse für Risikoanalyse, Risikoüberwachung oder Risikoreporting). Ob die hier genutzten Methoden aber überhaupt geeignet sind, um den (gesetzlichen) Anforderungen und Zielen des Risikomanagements gerecht zu werden, wurde mit weniger Intensität betrachtet.

Von besonderer Bedeutung sind u.a. folgende Aspekte des DIIR RS Nr. 2:

1. Das Risiko wird verstanden als Überbegriff zu möglichen positiven Abweichungen (Chancen) und negativen Abweichungen (Gefahren, Risiken im engeren Sinn). Die Einbeziehung der Chancen ist notwendig, um bei der Vorbereitung unternehmerischer Entscheidungen die hier bestehenden Hand-

lungsoptionen (z.B. Investitionen) nicht einfach „schlecht zu rechnen". Eine Vernachlässigung der potenziellen positiven Planabweichungen führt zu einer zu pessimistischen Betrachtung des gesamten Risikoumfangs eines Unternehmens. Dies hat erhebliche Auswirkungen in Bezug auf den Abgleich mit der vorhandenen Risikotragfähigkeit.

2. Mit Bezug auf die gesetzliche Anforderung aus § 91 Abs.2 AktG im Hinblick auf die Erkennung möglicher „bestandsgefährdender Entwicklungen" wird die Methode zur Risikoaggregation zum zentralen Prüfungsfeld, weil nur so durch diese erreicht werden kann, dass auch mögliche bestandsgefährdende Entwicklungen aus Kombinationseffekten von Einzelrisiken erfasst werden.
3. Der DIIR Revisionsstandard Nr. 2 betont zudem die Notwendigkeit der Quantifizierung von Risiken (ganz auf Linie des IDW PS 340) und empfiehlt die darauf aufbauende Messung der Risikotragfähigkeit und Risikotoleranz (wie auch IDW PS 981). Eine reine qualitative Bewertung von Risiken – wie in der Praxis nicht unüblich – ermöglicht keinerlei Aussage über „bestandsgefährdende Entwicklungen" und keine Abwägung der vorhandenen Risikotragfähigkeit zum aggregierten Risikoumfang.
4. Der DIIR Revisionsstandard Nr. 2 hebt hervor, dass es zu den Aufgaben des Risikomanagements gehört, sicherzustellen, dass schon bei der Vorbereitung wesentlicher unternehmerischer Entscheidungen deren Implikationen für den zukünftigen Risikoumfang nachvollziehbar aufgezeigt werden, um auch potenzielle bestandsgefährdende Entwicklungen früh zu erkennen.
5. Gemäß DIIR Revisionsstandard Nr. 2 sind alle Managementsysteme, z.B. auch des Controllings oder des Qualitätsmanagements einzubeziehen, wenn sie sich mit Chancen und Gefahren befassen.
6. Der DIIR Revisionsstandard Nr. 2 stellt klar, dass das wesentliche Ziel der Risikoberichterstattung und -kommunikation darin besteht, dass Entscheidungsträger und Aufsichtsrat zeitnah über die Risikolage der Organisation informiert werden.

IV. Fazit

Im Ergebnis wird aus der Business Judgement Rule ein Sachverhalt klar: Unternehmerische Entscheidungen sind immer mit Risiken verbunden. Kein Vorstand haftet für das „Pech", das die mit seinen Entscheidungen – z.B. bezüglich Investitionen oder Produktneuentwicklungen – verbundenen Risiken sich auch einmal realisieren können (und Verluste zur Konsequenz haben). Sorgfaltspflichtverletzungen liegen aber dann vor, wenn „unternehmerische Entscheidungen" nicht auf angemessenen Informationen basieren, also insbesondere in den Entscheidungsvorlagen nicht klargestellt wird, welche Chancen und Gefahren mit der Entscheidung verbunden sind.

Notwendig ist zudem, dass diese angemessenen Informationen mit angemessenen und geeigneten Methoden generiert wurden.

Aus der Business Judgement Rule (§ 93 AktG) und den Präzisierungen der Anforderung an das Risikomanagement im neuen Standard DIIR RS Nr. 2 des Instituts für interne Revision wird bei vielen Unternehmen eine Weiterentwicklung des Risikomanagements erforderlich. Notwendig ist insbesondere eine entscheidungsorientierte Ausrichtung des Risikomanagements, d.h. organisatorisch muss sichergestellt sein, dass schon bei der Vorbereitung „unternehmerischer Entscheidungen" durch eine Risikoanalyse aufgezeigt wird, welche Veränderung des Risikoumfangs sich durch diese Entscheidung ergeben würde.

Folgende zentrale Fragen sind zu beantworten:

1. Ist präzise definiert, was unter einer „unternehmerischen Entscheidung" zu verstehen ist (und was nicht)?
2. Ist organisatorisch sichergestellt, dass keine „unternehmerischen Entscheidungen" getroffen werden ohne adäquate Entscheidungsvorlagen?
3. Ist definiert, welche Inhalte in einer Entscheidungsvorlage enthalten sein müssen, um von „angemessenen Informationen" (§ 93 AktG) ausgehen zu können?
4. Enthalten die Vorlagen für „unternehmerische Entscheidungen" insb. Angaben zu Ziel, Handlungsmöglichkeiten, Ausgangssituation, Annahmen, Prognosen und Risiken?
5. Werden zur Vorbereitung von Entscheidungen insb. dokumentierte Risikoanalysen durchgeführt, die zeigen, welche Änderungen des Risikoumfangs durch die Entscheidungen bedingt sind (§ 93 AktG)?
6. Ist sichergestellt, dass das Risikomanagement bei wesentlichen unternehmerischen Entscheidungen in die Entscheidungsvorbereitung involviert wird?
7. Gibt es geeignete Mechanismen, um die Neutralität von Entscheidungsvorlagen zu gewährleisten?
8. Werden alle Vorlagen für „unternehmerische Entscheidungen", inklusive der getroffenen Entscheidung, erfasst und archiviert? ■

Literaturhinweise:

- Deutsches Institut für Interne Revision e.V. (2018), DIIR Revisionsstandard Nr. 2: Prüfung des Risikomanagementsystems durch die Interne Revision, Version 2.0, 2018.
- Gleißner, W. (2017), Grundlagen des Risikomanagements, 3. Aufl., Vahlen Verlag München.
- Gleißner, W./Kimpel, R. (2019), Prüfung des Risikomanagements und der neue DIIR Revisionsstandard Nr. 2, in: ZIR, Heft 4/2019, S. 148-159.
- Romeike, F. (2018), Risikomanagement, Springer Verlag, Wiesbaden 2018.
- Eine ausführliche praxisorientierte Checkliste finden Sie unter http://hbfm.link/6729.

Autoren:

Prof. Dr. Werner Gleißner, Vorstand der FutureValue Group AG und Honorarprofessor für Betriebswirtschaftslehre, insb. Risikomanagement, an der TU Dresden. **Frank Romeike** ist Gründer des Kompetenzzentrums RiskNET – The Risk Management Network. Er ist Geschäftsführer und Eigentümer der RiskNET GmbH sowie von RiskNET Advisory & Partner.