Veröffentlicht in

Der Aufsichtsrat

Heft 2/2018

Gleißner, W. (2018):

„Prüfung des Risikomanagements – ein Reifegradmodell“, S. 18 – 21

Mit freundlicher Genehmigung der
Handelsblatt Fachmedien GmbH, Düsseldorf

http://www.aufsichtsrat.de

»AR1258089

Prüfung des Risikomanagements – ein Reifegradmodell

Prof. Dr. Werner Gleißner

Das Risikomanagement ist von grundlegender Bedeutung, um „bestandsgefährdende Entwicklungen" (§ 91 AktG) früh erkennen zu können. Es ist zudem notwendig, um auch dem Aufsichtsrat zu zeigen, welche Veränderung von Ertragsrisiko und Rating mit anstehenden Entscheidungen verbunden ist. Der Aufsichtsrat sollte sich nicht allein auf die Prüfung des Risikofrüherkennungssystems durch einen Wirtschaftsprüfer verlassen. In diesem Beitrag werden Kriterien und Prüfungsfragen vorgestellt, mit denen sich ein Aufsichtsrat – im Gespräch mit Vorstand und Risikomanager – einen eigenen Eindruck von der Leistungsfähigkeit des Risikomanagements verschaffen kann.

I. Risikomanagement: Grundlagen und Status

Die Fähigkeiten eines Unternehmens im Umgang mit Chancen und Gefahren (Risiken) – und damit das Risikomanagement – sind von großer Bedeutung für den Unternehmenserfolg. Es trägt potenziell zur Senkung von Risikokosten bei, hilft, die Wahrscheinlichkeit bestandsbedrohender Krisen (oder gar einer Insolvenz) zu reduzieren und stellt Risikoinformationen bereit, um bei der Vorbereitung unternehmerischer Entscheidungen erwartete Erträge und Risiken gegeneinander abzuwägen. Der Aufsichtsrat muss sich daher im Rahmen seiner Überwachungspflichten intensiv mit dem Risikomanagement befassen.

Seit dem Inkrafttreten des Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) im Jahr 1998 fordert § 91 Abs. 2 AktG: „Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden." In seinem Prüfungsstandard IDW PS 340 führt das Institut der Wirtschaftsprüfer aus, was die Anforderungen an ein Risikofrüherkennungssystem sind: „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."

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.

Auch im Zusammenhang mit der „Business Judgement Rule" (§ 93 Abs. 1 Satz 2 AktG) ist ein funktionierendes Risikomanagement wichtig. Um bei unternehmerischen Entscheidungen „auf der Grundlage angemessener Information" zu handeln, müssen insbesondere auch Risikoinformationen bereitgestellt werden, d.h. eine Risikoanalyse sollte schon vor der Entscheidung durchgeführt werden.

In einer aktuellen Studie der FutureValue Group AG wurden die Risikoberichte der Unternehmen aus DAX und MDAX analysiert. Bei vielen Unternehmen muss demnach bezweifelt werden, ob bestandsgefährdende Entwicklungen auch aus der Kombinationswirkung mehrerer Einzelrisiken erkannt werden können. Die dafür notwendige Risikoaggregation wird nämlich offenbar bei vielen Unternehmen gar nicht durchgeführt.

II. Prüfung der Leistungsfähigkeit des Risikomanagements: Drei Strategien

Im Rahmen seiner Überwachungspflichten muss sich der Aufsichtsrat (zumindest der Prüfungsausschuss) ein eigenes Bild von der Leistungsfähigkeit des Risikomanagements verschaffen. Es existieren drei sich ergänzende Strategien für eine schnelle und effiziente Prüfung des Risikomanagements, die ein Aufsichtsrat selbst anwenden kann:

1. die Systemprüfung, die formale Anforderungen an das Risikomanagementsystem prüft,
2. die Output-Prüfung, die hinterfragt, ob dem Aufsichtsrat vom Vorstand diejenigen Informationen angeboten werden, die ein Risikomanagementsystem liefern sollte, und
3. die Abweichungsanalyse, die überprüft, ob eingetretene Planabweichungen auf im Vorhinein bekannte Risiken zurückgeführt werden können.

Orientiert an den Anforderungen des IDW PS 340 wird z.B. bei einer **Systemprüfung** hinterfragt, ob

- im Unternehmen geeignete Prozesse existieren, die neu auftretende Risiken systematisch identifizieren,
- wesentliche bekannte Risiken durch klar beschriebene Arbeitsprozesse kontinuierlich überwacht werden,
- die wesentlichen Risiken quantitativ bewertet und im Hinblick auf ein definiertes Risikomaß verglichen werden,
- die Einzelrisiken zu einer Gesamtrisikoposition (z.B. Eigenkapitalbedarf) aggregiert werden,
- die Berichtswege definiert sind, auf denen die wesentlichen Risikoinformationen an das zentrale Risikocontrolling, den Vorstand und – in verdichteter Form – an den Aufsichtsrat weitergeleitet werden,
- das Risikomanagementsystem und die wesentlichen Ergebnisse des Risikomanagements (z.B. Risikoinventar) adäquat dokumentiert sind sowie
- das Risikomanagement als Ganzes regelmäßig einer unabhängigen Prüfung unterzogen wird.

Bei der **Output-Prüfung** betrachtet der Aufsichtsrat, ob er im Reporting und speziell in den Entscheidungsvorlagen adäquat mit Risikoinformationen versorgt wird. Zu untersuchen ist, an welcher Stelle Risikoinformationen tatsächlich in wesentliche Entscheidungen (z.B. Investitionen, Finanzierungsentscheidungen oder Akquisitionen) eingeflossen sind. Dies ist nötig, um im Sinne der Business Judgement Rule (§ 93 Abs. 1 Satz 2 AktG) „angemessene Informationen" bei der Entscheidungsvorbereitung belegen zu können.

Ein weiterer Test der Leistungsfähigkeit des Risikomanagements ist die **Abweichungsanalyse**: Für alle wesentlichen Planabweichungen eines Unternehmens wird hinterfragt, ob die diesen zugrunde liegenden Ursachen tatsächlich im Vorhinein bereits als Risiken bekannt waren. Ein Risiko beschreibt definitionsgemäß die Möglichkeit einer Planabweichung, was Gefahren (mögliche negative Planabweichungen) und Chancen (mögliche positive Planabweichungen) umfasst. Eingetretene Planabweichungen (bzw. die ermittelten Ursachen) systematisch zu erfassen, ist damit ein effektiver Weg, neue Risiken zu identifizieren.

III. Reifegradmodell für die risikoorientierte Unternehmensführung: Prüffragen

Für die oben erwähnte Systemprüfung benötigt der Aufsichtsrat konkrete Prüfkriterien bzw. Prüffragen, die er (schriftlich oder mündlich) an seinen Vorstand stellen kann. Nachfolgend wird ein 6-Stufen-Reifegradmodell für eine Systemprüfung vorgestellt, das insgesamt die Risikomanagementfähigkeit eines Unternehmens betrachtet, speziell im Hinblick auf

1. die Erfüllung gesetzlicher Anforderungen und
2. den erreichten ökonomischen Nutzen.

Schon zur Erfüllung gesetzlicher Mindestanforderungen, die im „Streitfall" erfahrungsgemäß konsequent geprüft werden, sollte der Aufsichtsrat auf die Einhaltung zumindest der Anforderungen auf Stufe 3 hinwirken. Wünschenswert ist darüber hinaus, dass das Risikomanagement möglichst weitgehend auch die Kriterien der Stufe 4 erfüllt. Erst auf Stufe 4 ist nämlich gewährleistet, dass das Risikomanagement einen ökonomischen Mehrwert bietet (z.B. durch die Reduzierung von Risikokosten und die Bereitstellung von Informationen z.B. für die Investitionsbewertung).

> » Der Aufsichtsrat selbst sollte orientiert an konkreten Prüfkriterien im Gespräch mit dem Vorstand die Leistungsfähigkeit des Risikomanagements einschätzen. «

1. Stufe 1: Kein Risikomanagement

Es existieren kein ausgeprägtes Risikobewusstsein und kein formalisiertes System zum Umgang mit Risiken. Eine Berücksichtigung von Risiken findet nur sporadisch statt.

2. Stufe 2: Schadensmanagement

Die Unternehmensführung ist sich der Existenz bestimmter Risiken, speziell wesentlicher Gefahren, bewusst und setzt punktuell Maßnahmen zur Abwehr dieser Gefahren ein. Dabei wird auf die Einhaltung gesetzlicher Regelungen wie Umweltschutz und Arbeitsschutz geachtet. Im Rahmen unternehmerischer Entscheidungen wird eine mögliche gravierende Gefahr diskutiert, ohne dass für diese Beurteilung ein spezifisches Instrument eingesetzt wird.

3. Stufe 3: Regulatorisches Risikomanagement („KonTraG-Risikomanagement")

Im Unternehmen existiert ein Risikofrüherkennungssystem, das sämtliche wichtigen Risiken kontinuierlich überwacht und in einem Risikoinventar zusammenfasst. Die wesentlichen Regelungen sind schriftlich erfasst, sodass insbesondere Umfang, Verantwortlichkeit und Turnus der Risikoüberwachung fixiert sind. Die wesentlichen (insbesondere operativen) Risiken werden jeweils individuell im Hinblick auf geeignete Risikobewältigungsstrategien diskutiert. Bei allen wesentlichen unternehmerischen Entscheidungen wird explizit über die damit verbundenen Risiken nachgedacht und sie werden – allerdings nicht formalisiert und quantifiziert – in betriebliche Entscheidungen (zum Beispiel bei Investitionen) mit einbezogen. Risiken werden oft nur einheitlich durch Schadenshöhe und Eintrittswahrscheinlichkeit beschrieben. Eine (einfache) Risikoaggregation wird durchgeführt, um zu prüfen, ob aus Kombinationseffekten von Einzelrisiken „bestandsgefährdende Entwicklungen" entstehen können (§ 91 Abs. 2 AktG/IDW PS 340).

Tab. 1: Kriterien zur Stufe 3 („regulatorische Mindestanforderungen“)

	Stufe 3: Regulatorisches Risikomanagement	erfüllt	teilweise erfüllt	nicht erfüllt
1	Sind Aufgaben und Verantwortlichkeiten im Risikomanagement klar zugeordnet?			
2	Sind alle Regelungen zu Identifikation, Quantifizierung und Überwachung von Risiken angemessen, wirksam und für Dritte nachvollziehbar dokumentiert?			
3	Werden geeignete Arten von Wahrscheinlichkeitsverteilungen für die Risikoquantifizierung genutzt (beispielsweise Dreiecksverteilung mit Mindestwert, wahrscheinlichstem Wert und Maximalwert für das Kostenwachstum)?			
4	Werden die existierenden Risikobewältigungsmaßnahmen im Rahmen der Risikoquantifizierung berücksichtigt?			
5	Gibt es ein geeignetes und einheitlich verwendetes Risikomaß, um einzelne Risiken quantitativ vergleichen und priorisieren zu können?			
6	Ist klar erläutert, was eine „bestandsgefährdende Entwicklung“ (§ 91 AktG) ist (z.B. Verletzung von Covenants)?			
7	Wird eine Risikoaggregation regelmäßig durchgeführt, um bestandsgefährdende Entwicklungen aus Kombinationseffekten von Einzelrisiken zu erkennen?			
8	Sind die Wege für ein effizientes internes Risikoreporting und die Risikokommunikation (mit Bezug auf geeignete Schwellenwerte) festgelegt?			
9	Gibt es eine adäquate Verfahrensweise bezüglich „Ad-hoc-Meldungen“ zu Risiken und ihren Wirkungen?			
10	Werden Unternehmensführung und Aufsichtsrat regelmäßig über Einzelrisiken und Gesamtumfang der Risiken informiert?			

Tab. 2: Kriterien zur Stufe 4 („entscheidungsorientiertes Risikomanagement“)

	Stufe 4: Ökonomisches Risikomanagement (entscheidungsunterstützend)	erfüllt	teilweise erfüllt	nicht erfüllt
1	Werden Chancen und Gefahren (Risiken) mit Bezug auf Planwerte betrachtet (Risiken als wesentliche Ursache einer Planabweichung)?			
2	Werden auch strategische Risiken erfasst und in der Unternehmensführung regelmäßig diskutiert, insbesondere Bedrohungen der Erfolgspotenziale?			
3	Sind bestehende (Management-)Systeme, beispielsweise Controlling, Treasury, QM, in die Risikoanalyse eingebunden?			
4	Wird die Risikoaggregation über mehrere Jahre im Kontext einer integrierten Unternehmensplanung durchgeführt, werden also Risiken den Positionen zugeordnet, bei denen sie Abweichungen auslösen können?			
5	Werden zur Vorbereitung von Entscheidungen des Vorstands dokumentierte Risikoanalysen durchgeführt, die zeigen, welche Änderungen des Risikoumfangs durch die Entscheidungen bedingt sind (§ 93 AktG)?			
6	Werden Einsatz und Nutzen von Risikobewältigungsmaßnahmen beurteilt und überwacht?			
7	Ist eine zur Unternehmensstrategie konsistente Risikopolitik formuliert, die den Rahmen von Risikomanagement und risikoorientierter Unternehmensführung beschreibt?			
8	Verfügt der Risikomanager über die notwendigen Kompetenzen, Ressourcen und Rechte (beispielsweise Informationsrecht über alle potenziell risikobehafteten Vorgänge wie beispielsweise geplante Akquisitionen oder Investitionen)?			
9	Werden die Implikationen der Risikoanalysen für Finanzierungsstruktur (Eigenkapitalbedarf) und angemessene Fremdkapitalkonditionen ausgewertet?			
10	Wird Risiko im Rahmen der Strategiefindung als wesentlicher Aspekt bei der Auswahl strategischer Handlungsoptionen betrachtet (Ziel: robuste Strategie)?			

4. Stufe 4: Ökonomisches entscheidungsorientiertes Risikomanagement

Aus den Einzelrisiken wird mittels Risikoaggregation unter Bezugnahme auf eine integrierte Unternehmensplanung ein Gesamtrisikoumfang berechnet, aus dem z.B. der Eigenkapitalbedarf zur Deckung möglicher risikobedingter Verluste abgeleitet werden kann (Monte-Carlo-Simulation). Die Wirkungen auf das zukünftige Rating – ein Maß für den „Grad der Bestandsgefährdung" – und Covenants werden untersucht und die Risikotragfähigkeit berechnet. Fundierte Risikoinformationen werden in Entscheidungsvorlagen für Vorstand und Aufsichtsrat dargestellt. Aussagen über die Veränderung des Gesamtrisikoumfangs (und des Ratings) durch eine Vorstandsentscheidung sind notwendig, um über die vom Gesetz geforderten „angemessenen Informationen" bei Entscheidungsvorlagen verfügen zu können (§ 93 Abs. 1 Satz 2 AktG).

Das Ziel auf der vierten Entwicklungsstufe ist, Risikomanagement, Controlling und Strategieentwicklung zu verbinden, um ein „robustes Unternehmen" zu realisieren, das so flexibel und beweglich ist, sich auch an unvorhergesehene Entwicklungen anpassen zu können.

5. Stufe 5: Integriertes wertorientiertes Risikomanagement

Der Risikomanagement-Prozess und die unterstützenden Instrumente (z.B. IT) sind mit den operativen Systemen des Unternehmens verbunden. Planung wird im Sinne einer „stochastischen Planung" (stochastische Budgetierung) durchgeführt, d.h. alle Planungen können durch Zuordnung von Risiken beschrieben werden („Bandbreitenplanung"). Damit wird die Beurteilung der Planungssicherheit aller wesentlichen Planungspositionen möglich. Risikoinformationen in Unternehmen können genutzt werden, um den Wertbeitrag (Erfolgsmaßstab aus Verdichtung von erwarteten Erträgen und Risiken) zu berechnen, was eine am Unternehmenswert orientierte Optimierung der Risikobewältigung ermöglicht. Das Rating wird als risikoabhängiger Werttreiber verstanden, der langfristig etwa wie eine „negative Wachstumsrate" auf den Unternehmenswert wirkt („Insolvenzrisiko"). Der Kapitalkostensatz, der die risikogerechte Mindestanforderung an die erwartete Rendite ausdrückt, wird aus dem Ertragsrisiko (Cash-flow-Volatilität), einem Ergebnis der Risikoaggregation, abgeleitet (und nicht mehr aus historischen Aktienrenditeschwankungen wie meist beim Beta-Faktor des Capital Asset Pricing Model). Eine „robuste Strategie" wird umgesetzt.

6. Stufe 6: Embedded Risikomanagement (holistisch)

Bei allen wesentlichen Entscheidungen, nicht nur Vorstandsentscheidungen, erfolgt ein Abwägen erwarteter Erträge und Risiken bei der Entscheidungsvorbereitung. Sämtliche wichtigen strategischen und operativen Entscheidungen werden dabei durch Bewertung am risikogerechten Ertragswert beurteilt. Jedes Management wird wegen der unsicheren Auswirkungen von Entscheidungen und Handlungen auch als Risikomanagement aufgefasst. Eine ausgeprägte Risikokultur führt dazu, dass sich entsprechend alle Mitarbeiter mit den mit ihrer Arbeit verbundenen Chancen und Gefahren (Risiken) sach- und stufengerecht befassen.

IV. Fazit

Risikomanagement ist weit mehr als ein formales Organisationssystem, eher ein Kompetenzfaktor und ein Erfolgsfaktor. Es ist derjenige Kompetenzbereich, der – verteilt auf eine Vielzahl von Mitarbeitern und Funktionen – die Unternehmensführung in die Lage versetzt, erwartete Erträge und Risiken gegeneinander abzuwägen und so die Idee eines wertorientierten Managements in der Praxis umzusetzen. Diese Fähigkeit wird aber erst auf der vierten der oben erläuterten Stufen erreicht und auch hier gibt es noch weitere Verbesserungspotenziale. Insbesondere der Vorstand sollte sich selbst als „oberster Risikomanager" verstehen, da seine Entscheidungen den Risikoumfang maßgeblich bestimmen und grundlegende Änderungen des Ertrag-Risiko-Profils meist Anpassungen der Strategie erfordern. Empfehlenswert sind „robuste" Strategien sowie organisatorische Regelungen und Methoden, die sicherstellen, dass schon bei der Vorbereitung unternehmerischer Entscheidungen deren Implikationen für den zukünftigen Risikoumfang bekannt sind.

Der Aufsichtsrat erhält bei einem entscheidungsorientierten Risikomanagement in den Entscheidungsvorlagen für zustimmungspflichtige Geschäfte auch nachvollziehbare Informationen, wie sich diese auf den aggregierten Gesamtrisikoumfang (Eigenkapitalbedarf) und das zukünftige Rating des Unternehmens auswirken. Um ein dafür notwendiges leistungsfähiges Risikomanagementsystem zu gewährleisten, sollte er sich nicht allein auf das Testat des Wirtschaftsprüfers verlassen. Mit den in diesem Beitrag erläuterten Prüfkriterien und Fragen kann er sich – im Gespräch mit dem Vorstand – selbst schnell ein Bild von der Leistungsfähigkeit des Risikomanagements verschaffen (und Anstöße für notwendige Verbesserungen geben). ■

Literaturhinweise:

- Gleißner, Entscheidungsvorlagen für den Aufsichtsrat: Fallbeispiel Akquisition, „Der Aufsichtsrat" 2017, S. 54-57.
- Gleißner, Robuste Unternehmen und strategisches Risikomanagement, Risiko Manager 02/2017, S. 20-28.
- Gleißner, Grundlagen des Risikomanagements, 3. Aufl., Vahlen: München 2017.
- Gleißner, Reifegradmodelle und Entwicklungsstufen des Risikomanagements: ein Selbsttest, Controller Magazin 06/2016, S. 31-36.
- Gleißner, Der Vorstand und sein Risikomanager. Dreamteam im Kampf gegen die Wirtschaftskrise, UVK Verlag: Konstanz/München 2015.
- Graumann/Grundei, Nachweis einer „angemessenen Information" im Sinne der Business Judgement Rule, ZCG 2015, S. 197-204.
- Romeike (Hrsg.), Rechtliche Grundlagen des Risikomanagements, ESV: Berlin 2008.

Autor:
Prof. Dr. Werner Gleißner, Vorstand der FutureValue Group AG und Honorarprofessor für Betriebswirtschaftslehre, insbesondere Risikomanagement, an der TU Dresden.