Veröffentlicht in

Controlling

Heft 4/2020

Gleißner, W. (2020):

„Integratives Risikomanagement – Schnittstellen zu Controlling, Compliance und Interner Revision“,

S. 23 – 29

Integratives Risikomanagement

Schnittstellen zu Controlling, Compliance und Interner Revision

Sämtliche unternehmerische Aktivitäten sind mit Chancen und Gefahren (Risiken) verbunden. Daher ist ein integrativer Risikomanagementansatz zu wählen, der Risikomanagement mit allen Unternehmensfunktionen verknüpft. Risikomanagement sollte in den Prozess der Vorbereitung „unternehmerischer Entscheidungen“ integriert werden; diskutiert wird daher die Verbindung zu Controlling und Interner Revision.

Werner Gleißner

Prof. Dr. **Werner Gleißner** ist Honorarprofessor an der TU Dresden (BWL, insbesondere Risikomanagement) und Vorstand der *FutureValue Group* AG, Leinfelden-Echterdingen, sowie Vorstand der *EACVA*.

1. Die Idee eines integrativen Risikomanagements

Controlling, Risikomanagement und interne Revision sind wesentliche Teile des Managementsystems eines Unternehmens, die vielfältige Verknüpfungspunkte aufweisen. Es gibt Unternehmen, die Risikomanagement und Controlling weitgehend eigenständig organisiert haben und solche, die ein hohes Maß an Integration erreicht haben. Ähnlich verhält es sich mit der internen Revision.

Dieser Beitrag diskutiert die Stellung von Risikomanagement, Controlling, Compliance und interner Revision. Die Diskussion geht dabei insbesondere von den jüngst präzisierten Anforderungen an ein „entscheidungsorientiertes Risikomanagement“ aus, die sich aus den gesetzlichen Regelungen zur Business Judgement Rule (§ 93 AktG) ableiten lassen, und seit November 2018 erstmalig in einem Standard erfasst wurden (dem *DIIR* RS Nr. 2 des *Deutschen Instituts für interne Revision*).

2. Integratives Risikomanagement: Begriff und Bedeutung der Entscheidungsorientierung

Der Begriff des „integrativen Risikomanagements“ ist nicht einheitlich belegt. In diesem Beitrag wird von einem integrativen Risikomanagement gesprochen, wenn es mindestens eine von zwei Anforderungen erfüllt:

1. Das Risikomanagement ist verknüpft mit anderen Managementsystemen, tauscht mit diesen Daten aus und kann auch auf Ressourcen dieser Managementsysteme zur Erfüllung der eigenen Aufgaben zurückgreifen (Dimension 1).
2. Das Risikomanagement ist integriert in die Vorbereitung von Managemententscheidungen, d. h. es analysiert, wie sich durch diese der Risikoumfang des Unternehmens verändern würde (Dimension 2).

Es wird nachfolgend als Mindestanforderung für ein gesetzeskonformes, integratives Risikomanagement angesehen, dass es entscheidungsorientiert ist, also zumindest bei „unternehmerischen Entscheidungen“ Risikoinformationen bereitstellt. Über diese Mindestanforderungen hinaus hängt der „Integrationsgrad“ davon ab, inwieweit das Risikomanagement bei seiner Aufgabe sinnvoll mit anderen Managementsystemen interagiert, also insbesondere Informationen austauscht und Ressourcen anderer Systeme nutzen kann.

Ein entscheidungsorientiertes Risikomanagement (vgl. *Gleißner*, 2015) ist immer auch integrativ, was auch die jüngste Version des COSO Enterprise Risk Management-Standards (2017) verdeutlicht: Integration und Entscheidungsorientierung sind dort die zentralen neuen Gedanken (vgl. *Hunziker*, 2019). Ähnliche Überlegungen findet man auch im Risk Governance-Ansatz (vgl. *Stein/Wiedemann*, 2016). Da der zentrale Treiber für ein integratives Risikomanagement die Business Judgement Rule ist, seien deren Anforderungen zunächst knapp skizziert.

Durch die Rechtsprechung wurden in den letzten Jahren die Anforderungen an die Vorbereitung „unternehmerischer Entscheidungen“ (§ 93 AktG) präzisiert (vgl. *RMA*, 2019). Der Gesetzgeber stellt klar, dass kein Vorstand und kein Geschäftsführer für „Pech“ haftet. Unternehmertum ist unvermeidlich mit dem Eingehen von Risiken verbunden und diese können sich eben auch realisieren und zu negativen Planabweichungen, Verlusten oder gar zu einer

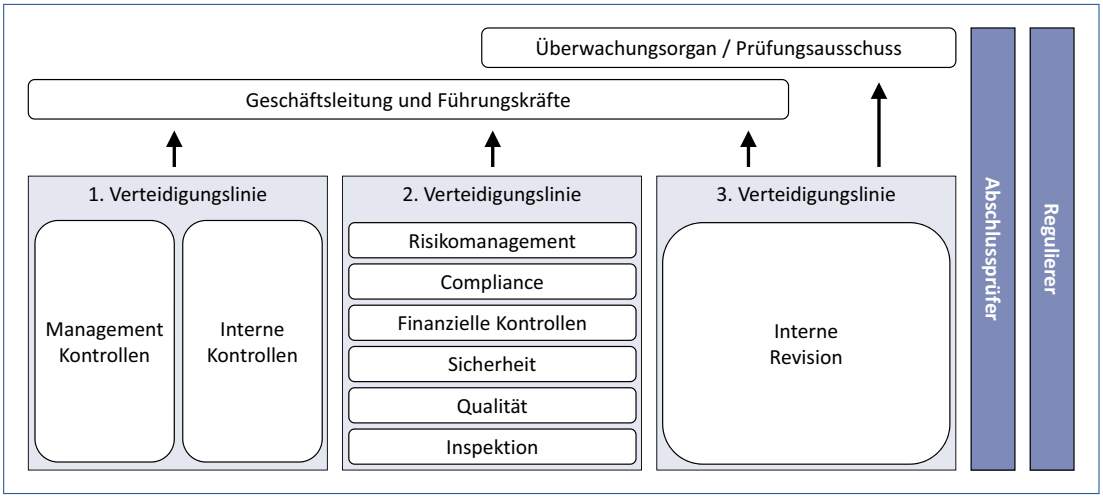

Abb. 1: Das Three-Lines-of-Defense-Modell (in Anlehnung an: *ECIIA/FERMA*, Guidance on the 8th EU Company Law Directive. Article 41, S. 9 und *IIA Position Paper*, Three Lines of Defence in Effective Risk Management and Control. January 2013, S. 2)

Das „Three-Lines-of-Defense-Modell" bietet einen Rahmen für ein integratives Risikomanagement.

Insolvenz führen. Vorstand und Geschäftsführer können und sollen nicht alle Risiken vermeiden. Aufgrund der Sorgfaltspflicht wird von der Geschäftsführung allerdings verlangt, dass sie schon vor einer unternehmerischen Entscheidung die mit dieser verbundenen Risiken betrachtet und insgesamt die Entscheidung basierend auf „angemessenen Informationen" trifft. Alle „unternehmerischen Entscheidungen" im Sinne § 93 AktG haben aufgrund bestehender Chancen und Gefahren (Risiken) unsichere Auswirkungen. Entsprechend ist es notwendig, dass die Entscheidungsvorlagen insbesondere darüber informieren

- Welche Veränderung des Risikoumfangs aus einer solchen Entscheidung resultiert und
- Wie diese Veränderung des Risikoumfangs im Entscheidungskalkül berücksichtigt wird („risikogerechte Bewertung", vgl. *Gleißner*, 2019).

Es ist zudem zu prüfen, ob durch die mit einer Entscheidung einhergehenden zusätzlichen Risiken „bestandsgefährdender Entwicklungen" (im Sinne § 91 Abs. 2 AktG) zu befürchten sind (vgl. *Graumann* et al., 2009 und *RMA*, 2019). Die entsprechenden Informationen sind aufgrund der im Gesetz formulierten Beweislast beim Vorstand zu dokumentieren.

Es ist traditionell insbesondere eine Aufgabe des Controllings, speziell des strategischen Controllings, Vorstände und Geschäftsführer bei der Vorbereitung solcher Entscheidungen zu unterstützen (z. B. durch eine Strategiebewertung). Aufgrund der zentralen Bedeutung von Risikoinformationen bei solchen Entscheidungen ist entsprechend ein enges Zusammenwirken von Controlling und Risikomanagement, also ein integrativer Risikomanagement-Ansatz, naheliegend.

3. Three Lines of Defense und die Verbindung von Risikomanagement zur Internen Revision und Compliance

Seit einiger Zeit wird das „Three-Lines-of-Defense-Modell" (TLoD, vgl. *Bantleon* et al., 2017) als Rahmenwerk für ein effektives internes Kontroll- und Überwachungssystem diskutiert, das die Aufgabenverteilung zwischen Internem Kontrollsystem (IKS), Risikomanagement, Controlling, Interner Revision und dem operativen Management eines Unternehmens thematisiert. Es kann als Rahmen für die Diskussion „integrativer Konzepte" dienen.

Man kann die „drei Verteidigungslinien" aus **Abb. 1** wie folgt beschreiben (*Bantleon* et al., 2017):

- Das operative Management als erste „Verteidigungslinie" ist verantwortlich für Identifikation, Quantifizierung und Überwachung von Risiken sowie die Initiierung von Risikobewältigungsmaßnahmen im Tagesgeschäft.
- Die zweite Verteidigungslinie umfasst Compliance, Controlling und Risikomanagement. Ihre Aufgabe ist primär das Bereitstellen von Methoden und Prozesse zum Umgang mit Chancen und Gefahren (Risiken), die Überwachung der risikobezogenen Aktivitäten der „ersten Verteidigungslinie" und die entscheidungsorientierte Aufbereitung von Risikoinformationen für die Unternehmensführung (inkl. Risikoaggregation).
- Die „dritte Verteidigungslinie" stellt die interne Revision als neutrale Stelle dar, die die Umsetzung der Vorgaben für die erste und zweite Verteidigungslinie überprüft und die Unternehmensführung, gegebenenfalls auch den Aufsichtsrat, über diese Prüfergebnisse informiert. Insbesondere der gesamte Prozess des Risikomanagements sollte von einer unabhängigen Instanz wie der internen Revision, regelmäßig überprüft werden (vgl. Anforderung aus *IDW* PS 340 und *DIIR* RS Nr. 2).

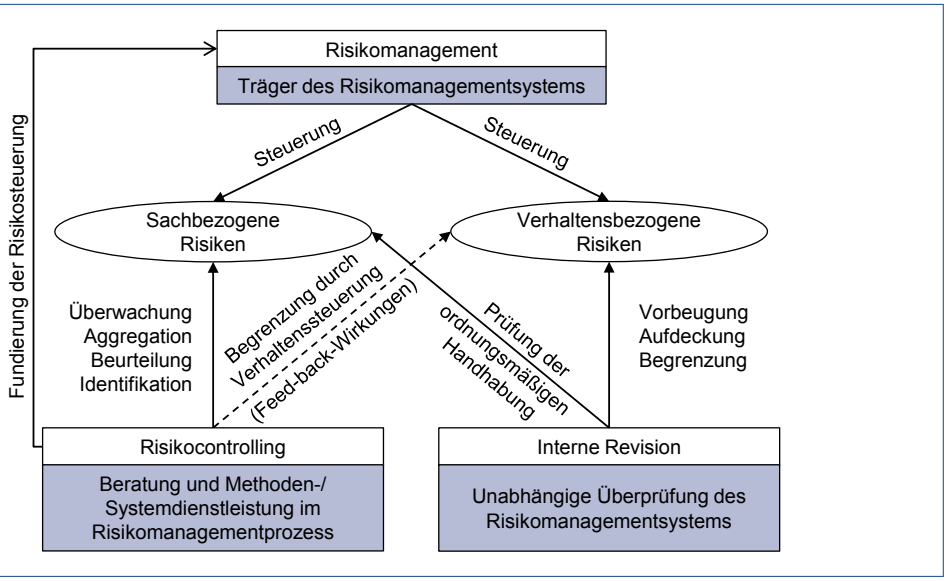

Abb. 2: Zusammenhang von Risikomanagement, Risikocontrolling und interner Revision (vgl. *Löhr*, 2010, S. 76)

Das interne Kontrollsystem ist auf der „ersten Linie". Aus Sicht des Risikomanagements ist das interne Kontrollsystem eine organisatorische Risikobewältigungsmaßnahme, die die Reduzierung der Eintrittswahrscheinlichkeit und Schadenshöhen durch operationelle Verhaltensrisiken der Mitarbeiter ermöglicht.

Das mögliche Zusammenspiel zwischen Risikomanagement, Risikocontrolling, als Teil des Controllings, und interner Revision verdeutlicht **Abb. 2** (vgl. *Löhr*, 2010, S. 121–130).

Die Interne Revision ist durch ihre Prüftätigkeit selbst ein Instrument für die Bewältigung einer wesentlichen Kategorie von Risiken: Der verhaltensbezogenen Risiken, also Risiken aus Fehlverhalten der Mitarbeiter (als eine Untermenge der operationellen Risiken). Sie ergänzt hier das interne Kontrollsystem. Die Interne Revision hat damit eine Doppelfunktion: Zum einen ist sie selbst Teil des Risikomanagements im weiteren Sinn. Zum anderen übernimmt sie oft die Prüfung des Risikomanagements. Eine Verknüpfung mit dem Risikomanagement, also der internen Revision, ist problematisch, weil durch diese die unabhängige Prüfung des Risikomanagements nicht mehr möglich ist (zumindest nicht intern). Da Risikomanagement und Controlling Teil der 2. Linie sind, ist eine enge Verknüpfung oder Integration prinzipiell einfacher möglich (vgl. Abschnitt 4). Eine Verknüpfung mit anderen Funktionen der Second Line of Defense, wie dem Compliance-System, ist möglich, aber nicht immer unproblematisch.

Die GRC-Ansätze sind in gewisser Weise integrativ, da sie – wie der Name sagt – Governance, Risk und Compliance verknüpft (vgl. *Scherer*, 2012). Die Denkweise von Compliance und eines entscheidungs- oder wertorientierten Risikomanagements sind aber nur teilweise kompatibel. Ein entscheidungsorientiertes Risikomanagement fasst Risiko als Schwankung um einen Erwartungswert auf, betrachtet als Chancen und Gefahren (vgl. *IDW* PS 981, ISO 9001: 2015 und *COSO* ERM: 2017). Sofern keine „bestandsgefährdenden Entwicklungen" mit relevanter Wahrscheinlichkeit auftreten, ist eine Erhöhung des Risikoumfangs sinnvoll (und wertsteigernd), wenn dem eine adäquate Erhöhung der erwarteten Erträge gegenübersteht. Risiko und Ertrag werden gegeneinander abgewogen. Die Denkweise von Compliance ist oft (noch) anders: Risiken sind Gefahren und werden als Ursache von Schäden durch die Verletzung von vorgegebenen Regeln (speziellen Gesetzen) aufgefasst. Zudem sieht man häufig die Vorstellung, dass Risiken – unabhängig von den damit entstehenden Kosten – zu vermeiden sind. Dies ist im Widerspruch zur betriebswirtschaftlichen Logik im Allgemeinen und einem wertorientierten Controlling im Besonderen. Tatsächlich ist es auch bei „Compliance-Risiken" nicht immer möglich diese sinnvoll zu minimieren oder gar auf null zu reduzieren. Die Integration von Risikomanagement und Compliance ist nur sinnvoll, wenn im Bereich Compliance die „Null-Risiko-Denkweise" aufgegeben wird.

Die Unabhängigkeit von Risikomanagement und interner Revision bringt Vorteile.

Fazit: Controlling und Risikomanagement haben im Rahmen der Three Lines of Defense als Komponenten der „zweiten Linie" die Aufgabe, Chancen und Gefahren (Risiken) zu erfassen und zu aggregieren und können gut verknüpft werden. Die Revision prüft das Risikomanagement und soll möglichst eigenständig bleiben (vgl. Anforderungen nach *IDW* PS 340).

4. Verknüpfung von Risikomanagement und Controlling

Risikomanagement und Controlling sind diejenigen Instanzen, die bei der Vorbereitung unternehmerischer Entscheidungen unter Risiko (Unsicher-

Zentrale Aussagen

- Ein integratives Risikomanagement dient der Vorbereitung „unternehmerischer Entscheidungen" (§ 93 AktG), was eine enge Zusammenarbeit mit dem Controlling erfordert, die Synergien erschließt.
- In Entscheidungsvorlagen muss gezeigt werden, wie sich der Risikoumfang eines Unternehmens infolge der unternehmerischen Entscheidungen verändern würde.
- Die Risikoaggregation (Monte-Carlo-Simulation) ist das Wichtigste gemeinsame Instrument für Controlling und Risikomanagement.
- Der *DIIR* RS 2 fordert eine entscheidungsorientierte Ausrichtung des Risikomanagements und eine Prüfung auch der Methoden für Risikoquantifizierung und Risikoaggregation.

heit) zusammenarbeiten sollten. Denn die Optimierung des Ertrag-Risiko- Profils und das damit notwendige Abwägen von Chancen und Risiken ist die zentrale Herausforderung jeglichen unternehmerischen Handelns bei einer nicht sicher vorhersehbaren Zukunft. Notwendig ist die Bewertung strategischer Optionen mithilfe von Verfahren, die Ertrag und Risiko gegenüberstellen (z. B. durch Berechnung des Unternehmenswerts als Performancemaß, vgl. *Gleißner*, 2019). Aus dieser Perspektive wird offensichtlich, dass der traditionelle Fokus des Risikomanagements auf Risiken, denen das Unternehmen bereits ausgesetzt ist, zu kurz greift. Um die entscheidungsorientierte Ausrichtung des Risikomanagements umzusetzen, bedarf es der Überwindung der Trennung zwischen Risikoanalyse und Entscheidungsprozessen.

Das Controlling kann viele Basisaufgaben des Risikomanagements gut abdecken.

Die Grundidee des integrativen Risikomanagements, das entscheidungsorientiert ist und Ressourcen des Controllings nutzt, basiert auf der Erkenntnis, dass Risiken immer mögliche Planabweichungen darstellen und damit deren Identifikation, Quantifizierung und kontinuierliche Überwachung weitgehend in der Planung und im Controlling-System verankert werden kann. Somit wird nach allen Möglichkeiten gesucht, die vorhandenen Managementsysteme (wie Planung, Controlling, Budgetierung, Treasury und Qualitätsmanagement) zu nutzen, um Aufgaben des Risikomanagements mit abzudecken oder zu unterstützen. Wesentliche Aufgaben des Risikomanagements können so effizient unmittelbar im Rahmen der Controlling-, Planungs- und Budgetierungsprozesse abgedeckt werden (vgl. *Gleißner/Kalwait*, 2017):

- **Nutzung von Planung und Budgetierung für die Risikoidentifikation:** Planwerte und Budgets basieren auf Annahmen, z. B. Entwicklung von Rohstoffpreisen. Immer wenn in der Planung eine unsichere Annahme erkannt wird, wird ein Risiko identifiziert. Daher ist es effizient schon im Planungsprozess solche risikobehafteten Annahmen explizit zu erfassen und diese Informationen dem Risikomanagement zur Verfügung zu stellen.
- **Risikoquantifizierung und Planung:** Sobald der Planwert (z. B. für ein Kostenbudget) festgelegt ist, kann zugleich angegeben werden, welche Risiken hier zu Planabweichungen führen und welchen Umfang diese haben können. So kann z. B. für eine Planungsposition Mindestwert, wahrscheinlichster Wert und Maximalwert angegeben werden (also eine Dreiecksverteilung, vgl. *Gleißner*, 2017, S. 174 ff.).
- **Identifikation von Risiken mittels Abweichungsanalyse:** Immer, wenn eine Planabweichung auf eine Ursache zurückzuführen ist, die bisher noch nicht im Risikomanagement erfasst ist, wird ein neues Risiko identifiziert.
- **Quantifizierung von Risiken auf Basis von Planabweichungen:** Mittels statistischer Analysen können Planabweichungen der Vergangenheit ausgewertet werden, um Risiken zu quantifizieren.
- **Integration von Risikobewältigungsmaßnahmen in die Unternehmenssteuerung:** Für unsichere Planungspositionen werden Maßnahmen initiiert, die zukünftigen Planabweichungen in ihrer Eintrittswahrscheinlichkeit oder ihrem quantitativen Umfang entgegenwirken.
- **Entscheidungsvorbereitung:** Bei der Vorbereitung einer Entscheidung werden Risikoanalysen durchgeführt.
- **Strategisches Risikocontrolling mit Balanced Scorecard:** Strategische Management- und Controllingsysteme (z. B. die Balanced Scorecard) werden genutzt, um die Unternehmensstrategie durch eine klare Beschreibung anhand von strategischen Zielen (Kennzahlen) sowie die Zuordnung von Maßnahmen und Verantwortlichkeiten operativ umzusetzen. Mit der Zuordnung von Risiken zu Kennzahlen, bei denen diese Planabweichungen auslösen können, wird eine Weiterentwicklung des traditionellen Balanced Scorecard-Ansatzes möglich (vgl. *Gleißner*, 2017). Der Vorteil einer derartigen Verbindung besteht einerseits in der höheren Effizienz, weil die Verantwortlichen für eine bestimmte Kennzahl zugleich für die Überwachung der zugehörigen Risiken verantwortlich werden. Die Übertragung der Verantwortung für die Risiken erhöht die Anreize, konsequent die Risiken zu identifizieren, die hier zu Planabweichungen führen können. Zudem wird bei einer Abweichungsanalyse eine verursachungsgerechte Zuordnung der Verantwortlichkeit für eingetretene Abweichungen möglich. Wirkungen „exogener" Risiken können i. d. R. den Verantwortlichen für die Kennzahl bei der Performance-Beurteilung nicht angelastet werden.

Die Übersicht zeigt, welche vielfältigen Ansatzpunkte es für einen integrativen Risikomanagementansatz gibt, der Risikomanagement und Controlling miteinander verbindet, ohne dass das Risikomanagement zwingend mit dem Controlling verschmolzen wird. Die zentrale Idee besteht darin, dass das Risikomanagement entscheidungsorientiert ausgerichtet ist und im Unternehmen bereits vorhandene Ressourcen, Prozesse und Tools, z. B.

für Planung und Budgetierung, für die eigenen Zwecke (mit) nutzen kann. Die Monte-Carlo-Simulation zur Risikoaggregation ist das wichtigste Tool, das Controlling und Risikomanagement gemeinsam nutzen sollten (vgl. *Gleißner*, 2017). Die gesetzlich vorgeschriebene Aufgabe für das Risikomanagement besteht gemäß § 91 AktG darin, mögliche „bestandsgefährdende Entwicklungen" früh zu erkennen. Da sich solche im Allgemeinen nicht aus Einzelrisiken, sondern aus Kombinationseffekten von Risiken ergeben, ist eine Risikoaggregation erforderlich. Bei dieser wird eine große repräsentative Anzahl risikobedingt möglicher Zukunftsszenarien berechnet, um ableiten zu können, mit welcher Wahrscheinlichkeit „bestandsgefährdende Entwicklungen" auftreten (z. B. durch Verletzung von Mindestanforderungen an das Rating oder die Verletzung von Covenants, die eine Kreditkündigung zur Folge haben können). Eine solche Risikoaggregation ist auch für Controlling und Entscheidungsvorbereitung wichtig, weil sie „erwartungstreue" Planwerte ableiten lässt (ambitionierte Zielwerte sind offensichtlich keine sinnvolle Entscheidungsgrundlage, vgl. *Gleißner*, 2008). Die Risikoaggregation über mehrere Planjahre führt zu einer Bandbreitenplanung, die Transparenz schafft über Planungssicherheit bzw. den Umfang möglicher Planabweichungen und die Ableitung risikoadäquater Kapitalkostensätze für die Investitions- und Strategiebewertung ermöglicht (vgl. z. B. *Gleißner*, 2019).

5. DIIR RS Nr. 2 als Rahmen für ein integratives Risikomanagement

Mit dem *DIIR* Revisionsstandard Nr. 2 des *Deutschen Instituts für Interne Revision* liegt erstmalig ein Standard vor, der die Anforderungen aus § 91 und § 93 AktG gemeinsam berücksichtigt und damit einen Rahmen für ein integratives Risikomanagement darstellt. Der *IDW* PS 340 befasst sich nur mit § 91 AktG (vgl. *Angermüller* et al., 2020).

Der *DIIR* RS Nr. 2 betont folgende Aspekte (in Anlehnung an *Gleißner/Kimpel*, 2019):

- Risiko wird verstanden als Überbegriff zu möglichen positiven Planabweichungen (Chancen) und negativen Planabweichungen (Gefahren, Risiken im engeren Sinn). Dies ist notwendig für ein entscheidungsorientiertes Risikomanagements, um erwartungstreue Planwerte zu erhalten.
- 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 erkannt werden.
- Der *DIIR* RS Nr. 2 betont die Notwendigkeit der Quantifizierung von Risiken (wie auch der *IDW* PS 340) und empfiehlt die darauf aufbauende Messung der Risikotragfähigkeit und Risikotoleranz (wie *IDW* PS 981).
- Der *DIIR* RS Nr. 2 hebt den strategischen Fokus des Risikomanagements hervor, ähnlich *COSO* Enterprise Risk Management (ERM) von 2017. Damit sind bei der Risikoidentifikation z. B. insbesondere auch strategische Risiken zu beachten (sowie unsichere Planannahmen).
- Entsprechend dem in Abschnitt 2 skizzierten Implikationen aus § 93 AktG wird ein „entscheidungsorientiertes Risikomanagement" gefordert (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."
- Während Risikobewältigung primär Aufgabe des operativen Managements ist, gibt es auch gemeinsame Aufgaben mit dem Risikomanagement. 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 (z. B. Risikocontrolling oder zentrales Risikomanagement)."
- Gemäß *DIIR* RS Nr. 2 sind zudem alle Managementsysteme, z. B. auch des Controllings oder des Qualitätsmanagements zu prüfen, wenn sie sich mit Chancen und Gefahren befassen. Dies zeigt den integrativen Ansatz.

Der *DIIR* Revisionsstandard 2 fordert wegen der Business Judgement Rule ein entscheidungsorientiertes Risikomanagement.

Im Ergebnis ist festzuhalten, dass der neue *DIIR* RS Nr. 2 durch seine Orientierung sowohl am § 91 wie auch am § 93 AktG den Rahmen für einen integrativen Risikomanagementansatz aufzeigt. Das Risikomanagement muss bei der Vorbereitung unternehmerischer Entscheidungen mitwirken, was zur Integration in den Prozess der Entscheidungsvorbereitung führt (und damit auch zu einem engen Zusammenspiel mit dem Controlling). Im Hinblick auf weitere organisatorische Integrationsmöglichkeiten bleibt der Standard offen und empfiehlt le-

Implikationen für die Praxis

- Controlling und Risikomanagement müssen bei der Vorbereitung „unternehmerischer Entscheidungen" (§ 93 AktG) zusammenarbeiten, um zu zeigen, wie sich der Risikoumfang infolge einer solchen Entscheidung verändern würde.
- Eine enge Verknüpfung von Risikomanagement und Controlling bietet viele Vorteile, z. B. kann Controlling bei der Erstellung der Planung durch das Aufzeigen unsicherer Annahmen Risiken identifizieren.
- Die interne Revision ist die Third Line of Defense und sollte unabhängig bleiben, um das Risikomanagement prüfen zu können.
- Der DIIR Revisionsstandards Nr. 2 (*von* 2018) ist ein geeigneter Standard für die Prüfung integrativer Risikomanagement-Ansätze und fordert eine Prüfung auch der Methoden für Risikoquantifizierung und Risikoaggregation.

diglich die Beachtung des Three-Lines-of-Defense-Modells. Die genaue Art des Zusammenspiels z. B. zwischen Risikomanagement und Controlling und der Umfang der Nutzung gemeinsamer Ressourcen, kann unternehmensindividuell geregelt werden.

6. Diskussion, Implikationen und Zusammenfassung

Controlling und Risikomanagement benötigen gemeinsame Methoden und Tools, insbesondere zur Risikoaggregation.

Es ist von einer Verletzung der gesetzlichen Sorgfaltspflichten von Vorständen und Geschäftsführern auszugehen, wenn diese bei „unternehmerischen Entscheidungen" nicht die dafür erforderlichen Informationen nachvollziehbar berücksichtigen (Business Judgement Rule, § 93 AktG). Um „angemessenen Informationen" vorliegen zu haben, ist insbesondere zu analysieren wie sich Chancen und Gefahren (Risiken) in Folge einer Entscheidung verändern würden. Dies erfordert eine Neuausrichtung vieler Risikomanagementsysteme, hin zu einem entscheidungsorientierten und mit auch integrativem Risikomanagement. Die Idee eines modernen, integrierten und entscheidungsorientierten Risikomanagements findet man inzwischen auch in aktuellen Risikomanagement-Standards, wie dem *COSO* Enterprise Risk Management (2017) und insbesondere dem *DIIR* RS Nr. 2 (2018). Ein integratives Risikomanagement bedeutet somit, dass das Risikomanagement zumindest in den Prozess der Vorbereitung „unternehmerischer Entscheidungen" integriert ist und möglichst eng mit anderen Unternehmensfunktionen verknüpft ist. Dies erfordert insbesondere Nähe zum Controlling, das traditionell die Instanz der Entscheidungsvorbereitung ist. Ob eine vollständige Übernahme von Risikomanagement-Aufgaben durch das Controlling angestrebt wird, oder Risikomanagement und Controlling lediglich eng aufeinander abgestimmt werden und Ressourcen gemeinsam nutzen, ist unternehmensspezifisch zu entscheiden. Es ist zu beachten, dass kein „eigenständiges" Risikomanagement mit eigenen Ressourcen gefordert ist. Notwendig ist es nur in geeigneter Weise zu erreichen, dass eben „bestandsgefährdende Entwicklungen" früh erkannt und bei „unternehmerischen Entscheidungen" „angemessene Informationen", inklusive derjenigen über die Risiken, vorliegen. Der Gesetzgeber spricht allgemein z. B. vom Überwachungssystem (im Sinne eines Managementsystems). Aus Sicht des Gesetzgebers ist damit jedes Managementsystem, das sich mit Chancen und Gefahren (Risiken) befasst, Teil des Risikomanagements. Im Extremfall kann ein integratives Risikomanagement also ein quasi virtuelles System ohne eigene Ressourcen darstellen. Die Aufgaben des Risikomanagements müssen dann von anderen Systemen, wie z. B. Controlling und Qualitätsmanagementsystemen, mit abgedeckt werden. Gerade das Controlling kann viele Aufgaben des Risikomanagements effizient abdecken, z. B. schon im Planungsprozess unsichere Planannahmen identifizieren und durch eine „Bandbreite" beschreiben.

Eine zu enge Verknüpfung des Risikomanagements mit der internen Revision ist problematisch, weil die Internen Revision – im Sinne des Three-Lines-of-Defense-Modells – für die unabhängige Überprüfung des Risikomanagements zuständig ist (vgl. auch *IDW* PS 340).

Literatur

- *Angermüller, N. O./Berger, Th. B./Blum, U./Erben, R. F./Ernst, D./Gleißner, W./Grundmann, Th./Heyd, R./Hofmann, K. H./Mayer, Ch./Meyer, M./Rieg, R./Schneck, O./Ulrich, P./Vanini, U.*, Gemeinsame Stellungnahme zum IDW EPS 340 (2020), https://www.idw.de/blob/121892/bdef576a6a3bff52ee039511482c6057/down-idweps340nf-gem-stn-hochschullehrer-rm-data.pdf, Stand 17.02.2020.
- *Bantleon, U./d'Arcy, A./Eulerich, M./Hucke, A./Knoll, M./Köhler, A./Pedell, B.* (Wissenschaftlicher Beirat des DIIR – Deutsches Institut für Interne Revision e. V.), Das Three-Lines-of-Defence-Modell: ein Beitrag zu einer besseren Corporate Governance? – Entstehung und Rezeption durch Standardsetzer und Regulatoren, in: WPg, 70. Jg. (2017), H. 12, S. 682 – 688
- *Gleißner, W.*, Erwartungstreue Planung und Planungssicherheit – Mit einem Anwendungsbeispiel zur risikoorientierten Budgetierung, in: Controlling, 20. Jg. (2008), H. 2, S. 81–87.
- *Gleißner, W.*, Controlling und Risikoanalyse bei der Vorbereitung von Top-Management-Entscheidungen – Von der Optimierung der Risikobewältigungsmaßnahmen zur Beurteilung des Ertrag-Risiko-Profils aller Maßnahmen, in: Controller Magazin, 40. Jg. (2015), H. 4, S. 4–12.
- *Gleißner, W.*, Grundlagen des Risikomanagements. Mit fundierten Informationen zu besseren Entscheidungen, 3. Aufl., München 2017.
- *Gleißner*, W., Risikomanagement 20 Jahre nach KonTraG: Auf dem Weg zum entscheidungsorientierten Risikomanagement, in: Der Betrieb, 71. Jg. (2018), H. 46, S. 2769–2774.
- *Gleißner, W.* (2019), Cost of capital and probability of default in value-based risk management, in: Management Research Review (MRR), 42. Jg., H. 11, S. 1243–1258.
- *Gleißner, W./Kalwait, R.*, Integration von Risikomanagement und Controlling – Plädoyer für einen völlig neuen Umgang mit Planungssicherheit im Controlling, in: *Gleißner, W./Klein, A.* (Hrsg.), Risikomanagement und Controlling, 2. Aufl., München 2017, S. 39–65.
- *Gleißner, W./Kimpel, R.*, Prüfung des Risikomanagements und der neue DIIR Revisionsstandard Nr. 2, in: ZIR, 7. Jg. (2019), H. 4, S. 148–159.
- *Graumann, M./Linderhaus, H./Grundei, J.*, Wann ist die Risikobereitschaft bei unternehmerischen

Entscheidungen „in unzulässiger Weise überspannt“?, in: BFuP, Jg. 2009, H. 5, S. 492–505.
- *Hunziker, S.*, Enterprise Risk Management – Modern Approaches to Balancing Risk and Reward, Wiesbaden 2019.
- *Löhr, B. W.*, Integriertes Risikocontrolling für Industrieunternehmen: Eine normative Konzeption im Kontext der empirischen Controllingforschung von 1990 bis 2009 (Controlling & Business Accounting), Frankfurt 2010.
- *Risk Management Association e. V. (RMA)* (Hrsg.), Managemententscheidungen unter Risiko, erarbeitet von Werner Gleißner, Ralf Kimpel, Matthias Kühne, Frank Lienhard, Anne-Gret Nickert und Cornelius Nickert, Berlin 2019.
- *Scherer, J.*, Good Governance und ganzheitliches strategisches und operatives Management: Die Anreichung des „unternehmerischen Bauchgefühls“ mit Risiko-, Chancen- und Compliancemanagement, in: Corporate Compliance Zeitschrift (CCZ), 5. Jg. (2012), H. 6, S. 201–211.
- *Stein, V./Wiedemann, A.*, Risk governance: Conceptualization, tasks, and research agenda, in: Journal of Business Economics, 86. Jg. (2016), H. 8, S. 813–836.

Literaturtipps aus dem Online-Archiv http://elibrary.vahlen.de

- Volker Hampel und Michael Bünis, Zusammenwirken von Controlling und Interner Revision im Three Lines of Defense-Modell der Unternehmensüberwachung, Ausgabe 11/2013, S. 596–601.
- Rainer Beaujean, Wolfram Stengel und Thomas Reichmann, Risikomanagement und Risiko-Controlling bei der Demag Cranes AG, Ausgabe 4–5/2012, S. 228–236.

Stichwörter

Business Judgement Rule # Compliance # Interne Revision # Risikomanagement # Three Lines of Defense

Keywords

Business Judgement Rule # Compliance # Internal Audit # Risk Management # Three Lines of Defense # Management Decisions

Summary

Decision-oriented risk management, as outlined by DIIR RS No 2, must support the preparation of business decisions leading to an integrated risk management. Further organizationally integration possibilities may be solved individually by company. A recommendation only exists for the Three-Lines-of-Defense-Model to be taken into account.