I.M.U.
Institut für Mitbestimmung
und Unternehmensführung

Das I.M.U. ist ein Institut
der Hans-Böckler-Stiftung

Wie überwacht der Aufsichtsrat wirksam?

RISIKOMANAGEMENT

Lars Beermann

August 2022

Das Risikomanagement stellt eine der zentralen Überwachungsinstanzen im Unternehmen dar, ist für den Aufsichtsrat jedoch zu häufig eine „Blackbox“. Dieser Kartenstapel bietet einen systematischen Überblick über den Aufbau und die Bestandteile dieser Systeme.

MITBESTIMMUNGS-
PORTAL

www.mitbestimmung.de/wissen-kompakt

Inhalt

1 Darum geht’s

Die kontinuierliche Überwachung der Unternehmensleitung und eine regelmäßige Überprüfung der Wirksamkeit des Risikomanagements (kurz: RMS) gehören zu den wesentlichen Aufgaben des Aufsichtsrats.

Der Aufsichtsrat ist damit mitentscheidend für die Wirksamkeit und Nachhaltigkeit von guter Corporate Governance.

Der Gesetzgeber hat diese Aufgaben konkretisiert und dabei insbesondere Unternehmen im Blick, die einen Prüfungsausschuss eingerichtet haben (vgl. § 107 Abs. 3 S. 2 AktG). Aber auch in Unternehmen ohne Prüfungsausschuss ist und bleibt das RMS eine Kernaufgabe des gesamten Aufsichtsrats.

Die Rolle des Aufsichtsrats ist dabei insbesondere darin zu sehen, die Maßnahmen und Informationen der Unternehmensleitung kritisch zu hinterfragen. Eine wirksame Überwachung durch den Aufsichtsrat setzt insbesondere angemessene Informationen in zeitlicher und inhaltlicher Hinsicht voraus.

Dieser Kartenstapel zeigt (aktuelle) Herausforderungen und praxisgerechte Lösungen auf, wie Aufsichtsratsmitglieder ihre gesetzliche Pflicht, die Wirksamkeit des RMS zu beurteilen, erfüllen können.

2 Allgemeines zum RMS

Auch wenn die tatsächliche Ausgestaltung und Umsetzung des RMS Aufgaben der Unternehmensleitung bleiben, ergeben sich auch für den Aufsichtsrat in diesem Zusammenhang nicht delegierbare Aufgaben.

Insbesondere Rahmenbedingungen, Aufbau und Wirksamkeit des RMS sowie deren laufende Überwachung fallen in das Aufgabenfeld des Aufsichtsrats. Es reicht insbesondere nicht aus, dass der Aufsichtsrat nur die Angemessenheit des RMS beurteilt.

Die Pflicht zur Einrichtung eines umfassenden RMS wurde bisher faktisch über die Sorgfaltspflichten eines ordentlichen und gewissenhaften Geschäftsleiters (§ 93 Abs. 1 AktG) hergeleitet. Auch die Pflicht zur Beurteilung der Wirksamkeit des RMS durch den Aufsichtsrat bzw. Prüfungsausschuss (§ 107 Abs. 3 S. 2 AktG) kann im Umkehrschluss nur bedeuten, dass die Unternehmensleitung ein solches einzurichten hat.

Lediglich die Einrichtung eines *Risikofrüherkennungssystems*, das aber nur Teilaspekte des *RMS* umfasst, war bis zum 10. Juni 2021 gemäß § 91 Abs. 2 AktG vorgeschrieben.

Diese „Lücke“ hat der Gesetzgeber mit dem Gesetz zur Stärkung der Finanzmarktintegrität vom 10. Juni 2021 (Finanzmarktintegritätsstärkungsgesetz – FISG) durch § 91 Abs. 3 AktG klarstellend zumindest für börsennotierte

Unternehmen geschlossen. Danach hat der Vorstand u. a. ein wirksames RMS einzurichten.

Was ist unter dem RMS zu verstehen?

Unter dem RMS ist die Gesamtheit aller Maßnahmen zur Erkennung, Beurteilung, Überwachung und Steuerung von Risiken und Chancen zu verstehen, die die Vermögens-, Finanz- und Ertragslage, und damit letztlich den Fortbestand des Unternehmens, beeinflusst. Dabei werden externe und interne Risiken gleichermaßen analysiert und ihre Auswirkungen auf das jeweilige Unternehmen beurteilt (siehe auch ➔I Praxisleitfaden zum DIIR Revisionsstandard Nr. 2 des Deutschen Instituts für Interne Revision).

Die Durchführung der Risikomanagementmaßnahmen wird durch Überwachungs- und Leitungsorgane gesteuert. Bereits bei der Festlegung der Unternehmensstrategie wird das Risikomanagement berücksichtigt, um mögliche Ereignisse zu erkennen, die im Falle eines Eintretens das Unternehmen beeinflussen.

Welche Unternehmen müssen ein RMS einrichten?

In § 91 Abs. 2 AktG wird die Pflicht für den Vorstand zur Einrichtung eines Risikofrüherkennungssystems geregelt. Hierdurch hat der Gesetzgeber die kodifizierte allgemeine Leistungsaufgabe des Vorstandes nach § 76 Abs. 1 AktG und die damit einhergehende geforderte Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters (§ 93 Abs. 1 AktG) konkretisiert. Gemäß § 93 AktG sind die Vorstandsmitglieder verpflichtet, unangemessen risikobehaftete Geschäfte, Verstöße gegen die Buchführungspflicht und Verstöße gegen gesetzliche Vorschriften zu unterlassen.

Mit Inkrafttreten des FISG zum 10. Juni 2021 und der damit neuen Vorschrift in § 91 Abs. 3 AktG müssen alle börsennotierten Unternehmen über ein wirksames Risikomanagement verfügen, das vom Vorstand einzurichten ist.

Spätestens mit dem zum 1. Januar 2021 in Kraft getretenen Unternehmensstabilisierungs- und -restrukturierungsgesetz (StaRUG) müssen darüber hinaus die zur Geschäftsführung berufenen Organe einer jeden juristischen Person (z. B. Geschäftsführer einer GmbH) fortlaufend über Entwicklungen wachen, welche den Fortbestand der juristischen Person gefährden können. Erkennen sie solche Entwicklungen, ergreifen sie geeignete Gegenmaßnahmen und erstatten den zur Überwachung der Geschäftsleitung berufenen Organen (Überwachungsorganen) unverzüglich Bericht (vgl. § 1 StaRUG).

Zusammenfassend bedeutet das, dass neben Aktiengesellschaften (s. a. § 91 Abs. 3 AktG) insbesondere auch GmbHs als weitere wesentliche Rechtsform ein Risikomanagementsystem (Aktiengesellschaften) bzw. ein Risikofrüherkennungssystem (z. B. GmbH) einzurichten haben. Bisher wurde die Pflicht dazu auch bei der GmbH nur über die allgemeinen Sorgfaltspflichten des Geschäftsführers und in Fällen, in denen ein Aufsichtsrat eingerichtet ist, über die Verweisvorschrift des § 52 GmbHG bzw. die

einschlägigen Verweise in den Mitbestimmungsgesetzen auf das Aktiengesetz argumentiert.

Die Anforderungen an diese Sorgfaltspflicht werden (auch) durch die sogenannte Business Judgement Rule (§ 93 Abs. 1 S. 2 AktG) festgelegt. Der Grundgedanke ist, dass unternehmerische Entscheidungen immer mit Risiken verbunden sind. Vorstände oder Geschäftsführungen verstoßen also nicht „automatisch“ gegen ihre Sorgfaltspflicht, wenn sie Risiken eingehen und diese im Falle ihres Eintretens auch zu einem Schaden für die Gesellschaft führen. Wenn die fünf Voraussetzungen (unternehmerische Entscheidung, Wohl der Gesellschaft, keine Sonderinteressen, angemessene Information und guter Glaube) der Business Judgement Rule erfüllt sind, ist die Sorgfaltspflicht nicht verletzt.

Das RMS spielt hierbei insbesondere in Bezug auf die angemessene Information eine wesentliche Rolle. Ist ein RMS nicht oder nicht in angemessener und wirksamer Form eingerichtet, können unternehmerische Entscheidungen, wie z. B. eine Investitionsentscheidung, in der Regel nicht auf Grundlage angemessener Information beschlossen werden können.

Was gilt in Tochtergesellschaften?

Wie dargestellt, fordert StaRUG nun von allen juristischen Personen die Früherkennung bestandsgefährdender Entwicklungen. In der Konsequenz müssen daher auch die Geschäftsführer von GmbHs, die als Tochtergesellschaft oft Teil eines Konzerns sind, sich selbst mit der Risikoanalyse und der Früherkennung befassen. Die RMS-Funktion in der „Konzern-Muttergesellschaft“ muss daher sicherstellen, dass das RMS auch auf Ebene der Tochter-GmbHs etabliert ist.

Die Geschäftsführer einer Tochter-GmbH können ihre Verantwortung, die direkt aus dem StaRUG resultiert, auch nicht delegieren, indem auf ein übergeordnetes „Konzern-RMS“ verwiesen wird.

3 Was ist der Unterschied zu Risikofrüherkennungssystemen?

In der Praxis ist zu beobachten, dass die Begriffe Risikomanagementsystem und Risikofrüherkennungssystem häufig synonym verwendet werden. Aber auch mit Blick auf die →| Aufgaben des Abschlussprüfers ist zu empfehlen, diese „scharf“ voneinander abzugrenzen.

Das Risikofrüherkennungssystem ist nur ein Teil des Risikomanagementsystems und umfasst grundsätzlich die Bereiche der Risikoidentifikation, der Risikobewertung und der Risikokommunikation. Ergänzend dazu umfasst das Risikomanagementsystem darüber hinaus noch die Bereiche der Risikosteuerung, der Risikokontrolle und die (Risiko-)überwachung.

4 Was sind Voraussetzungen für ein angemessenes RMS?

Ein grundsätzlich angemessenes RMS beruht im Wesentlichen auf:

– einem anerkannten Rahmenwerk (z. B. COSO-Rahmenwerk),

– unternehmens- bzw. konzernweit einheitlichen Vorgaben und Richtlinien,

– einer klaren und differenzierten Risikozielsetzung (z. B. Risikovermeidung) und

– einer kontinuierlichen Überwachung.

Eine wesentliche Herausforderung für den Aufsichtsrat ist in der Praxis, dass er (oft) abhängig von Informationen ist, die durch die Unternehmensleitung vorbereitet und dem Aufsichtsrat zur Verfügung gestellt werden.

Von besonderer Bedeutung für den Aufsichtsrat ist deshalb die interne Risikoberichterstattung, die die wesentliche Grundlage zur Beurteilung des RMS darstellt.

5 Welche Bestandteile hat ein RMS?

Der Prozess des Risikomanagements wird in der Theorie oft in acht Komponenten beschrieben, die in wechselseitiger Beziehung zueinanderstehen.

Bestandteile eines RMS sind:

– internes Umfeld (Risikophilosophie, Risikokultur und das Ausmaß der Risikobereitschaft),

– Risikoziele,

– Risikoidentifikation,

– Risikobeurteilung,

– Risikosteuerung

– Kontrollaktivitäten,

– Information und Kommunikation sowie

– Überwachung.

Komponenten des Risikomanagement-Prozesses

Der Prozess des Risikomanagements wird in der Theorie oft mit folgenden Komponenten beschrieben, die in wechselseitiger Beziehung zueinanderstehen. Das sind:

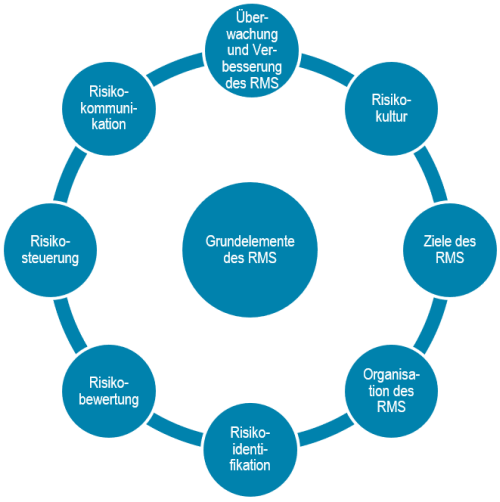
– Risikokultur,

– Ziele des RMS,

– Organisation des RMS,
– Risikoidentifikation,
– Risikobewertung,
– Risikosteuerung,
– Information und Kommunikation sowie
– Überwachung.

Die folgende Grafik verdeutlicht die Zusammenhänge der einzelnen Bestandteile:

Grundelemente des IDW PS 981



Quelle: Institut der Wirtschaftsprüfer (IDW)

Hans Böckler Stiftung

Risikokultur

Die Risikokultur ist ein wichtiger Teil der Unternehmenskultur. Sie umfasst die grundsätzliche Einstellung und die Verhaltensweisen beim Umgang mit Risikosituationen. Das bewusste Eingehen von Risiken ist inhärenter Bestandteil eines fast jeden wirtschaftlichen Geschäftsmodells und essenziell für die Erzielung von Erträgen.

Die Risikokultur beeinflusst damit maßgeblich das Risikobewusstsein im Unternehmen und bildet die Grundlage für ein wirksames RMS.

Der Begriff der Risikokultur ist nicht legal definiert. Risikokultur beschreibt die Rahmenbedingungen und kann sich z. B. darin äußern, bestimmte Märkte nicht zu bedienen, innerhalb derer die Mitarbeiter unternehmerische Entscheidungen treffen können.

Aspekte der Risikokultur sind daher also:

– Menschen,

– Verlustpotenzial,
– Handlungsrahmen und
– Risikoappetit.

Von besonderer Bedeutung ist dabei der sogenannte Risikoappetit, mit dem das bewusst gewählte und akzeptierte Maß an Risiken zur Erreichung des Unternehmensziels beschrieben wird. Der Risikoappetit ist der Rahmen für das Handeln der Unternehmensleitung in Bezug auf Entscheidungssituationen, die in der Regel immer mit Verlustpotenzialen für das Unternehmen verbunden sind.

Ziele des RMS

Ausgehend und nicht ganz trennscharf vom Begriff der Risikokultur abgrenzbar, wird unter den Zielen des RMS insbesondere die Festlegung einer Risikostrategie verstanden. Die Risikostrategie ist also Ausfluss der Risikokultur und konkretisiert den durch die Risikokultur festgelegten Rahmen (Bsp.: In der Risikostrategie wird festgelegt, dass Risiken – wenn möglich – priorisiert zu versichern sind).

In der Risikostrategie wird festgelegt, in welchem Ausmaß unter Berücksichtigung der Risikotragfähigkeit des Unternehmens Risiken eingegangen werden sollen (Risikoappetit). Ergänzt wird das durch unternehmenspolitische Vorgaben zum erwünschten Umgang mit Risiken in Form einer Risikopolitik bzw. in Form von risikopolitischen Grundsätzen. Risikopolitische Grundsätze können dabei z. B. dergestalt sein, dass man in bestimmten Branchen oder bestimmten Märkten grundsätzlich aktiv ist. Die Risikotragfähigkeit beschreibt die Fähigkeit der Gesellschaft, bis zu welchem Umfang Risiken getragen werden können. In der Praxis wird häufig das vorhandene Eigenkapital als Bezugsgröße zur Risikotragfähigkeit verwendet.

Die Zielfestlegung in Form einer Risikostrategie ist eine notwendige Voraussetzung, um Risiken zu identifizieren, zu beurteilen und steuern zu können. Ohne Zielfestlegung ist es nicht möglich zu beurteilen, ob beispielsweise die Risikosteuerung und initiierten Maßnahmen angemessen und wirksam sind.

Risikostrategien und -ziele können sich je nach Unternehmensgröße, Branche, Unternehmenskultur und Unternehmensphilosophie stark voneinander unterscheiden.

In der Gesamtbetrachtung sind die Ziele des RMS darauf ausgerichtet sicherzustellen, dass die Unternehmensziele entsprechend der Risikostrategie erreicht werden. Die konkrete Ausgestaltung und Umsetzung des RMS ist unter Beachtung der unternehmensspezifischen Besonderheiten vorzunehmen.

Wesentliche Zielsetzungen des RMS:

- Bestimmung einer Risikostrategie und Unterstützung der Unternehmensstrategie,
- Gewährleistung der Effektivität und Effizienz der Geschäftsprozesse,
- systematisches Nachhalten von Unsicherheiten, um frühzeitig geeignete Maßnahmen abzuleiten und Chancen zu nutzen,
- Sicherstellung der Verlässlichkeit der Berichterstattung an die entsprechenden Adressaten (z. B. Vorstand, Aufsichtsrat),
- Einhaltung der gültigen Gesetze und Vorschriften.

6 Wie werden Risiken und Chancen definiert?

Unternehmen sind einer Vielzahl von Risiken und Chancen ausgesetzt, welche die Erreichung der Unternehmensziele beeinflussen können. Risiken sind Ereignisse mit negativen Auswirkungen, die eine Wertschöpfung verhindern oder bestehende Vermögenswerte reduzieren können. Chancen sind Ereignisse, die das Erreichen von Zielen fördern und zur Wertschöpfung bzw. Werterhaltung beitragen. In Bezug auf die Unternehmensplanung kann auch gesagt werden: Risiken sind negative Planabweichungen, während Chancen positive Planabweichungen darstellen.

Risiken lassen sich dabei z. B. in finanzielle, rechtliche, leistungswirtschaftliche oder strategische Risiken unterteilen.

Erkennbar wird, dass Risiken auch in unterschiedlichen Kennzahlen bzw. Einheiten, z. B. erfolgsbezogen („Gewinnauswirkung“) oder liquiditätsbezogen, gemessen werden können. In der Praxis vorherrschend ist die erfolgsbezogene →| Messung von Risiken und Chancen.

Trotz der in der Praxis häufigen Fokussierung auf Risiken sollte beachtet werden, dass Risiken immer im Zusammenhang mit Chancen gesehen werden müssen, die auch Teil der (Konzern-)Lageberichterstattung nach § 289 Abs. 1 S. 5 HGB bzw. § 315 Abs. 1 S. 6 HGB sind. Risiken sind dabei nicht grundsätzlich „negativ“, da jede unternehmerische Entscheidung auch Risiken beinhaltet. Es ist auch nicht Hauptaufgabe des RMS, Risiken zu verhindern, sondern vielmehr, eine angemessene und wirksame Steuerung der Risiken sicherzustellen.

Praxistipp:

Die Risikodefinition macht den Zusammenhang zur Unternehmensplanung deutlich. Die Unternehmensplanung ist Ausgangspunkt und legt die (finanziellen) Unternehmensziele fest. Abweichungen von der Planung sind daher mit eingetretenen Risiken oder Chancen zu übersetzen. Ob das RMS wirksam ist, kann der Aufsichtsrat daher z. B. anhand von Planabweichungen versuchen zu beurteilen. Das RMS ist dann wirksam, wenn über die Ursachen von Planabweichungen frühzeitig in der internen Risikoberichterstattung berichtet wurde.

7 Wie lassen sich die Risiken identifizieren?

Der Prozess der Risikoidentifikation umfasst die strukturierte und detaillierte Erfassung aller möglichen Risiken der unternehmerischen Aktivitäten einschließlich ihrer Wirkungszusammenhänge. Die Risikoidentifikation hat in regelmäßigen Abständen zu erfolgen, damit die erfassten Informationen aktuell sind. Zur Risikoidentifikation können zahlreiche Instrumente eingesetzt werden, wie z. B. Bilanzsimulation, Szenariotechnik, Checklisten, Brainstorming, Brainwriting oder die Delphimethode.

Die Herausforderung in der Praxis besteht insbesondere darin, Signale (häufig auch „weak signals“) frühzeitig zu erkennen, die sich wesentlich auf die Geschäftstätigkeiten auswirken, um rechtzeitige Gegensteuerungsmaßnahmen einleiten zu können. In dieser Phase können Risiken oft noch nicht quantifiziert werden. Das Erkennen dieser Risiken bzw. dieser „weak signals“ muss daher Gegenstand der Analyse im Strategieprozess sein, wodurch deutlich wird, dass das RMS nicht als isolierter, sondern bereichsübergreifender Prozess verstanden werden muss.

Ein in diesem Zusammenhang häufig genanntes Negativbeispiel ist das Unternehmen Nokia, welches auf das Risiko aus dem technologischen Wandel von ursprünglichen Mobiltelefonen hin zu Smartphones viel zu spät reagiert hat.

Praxistipp:

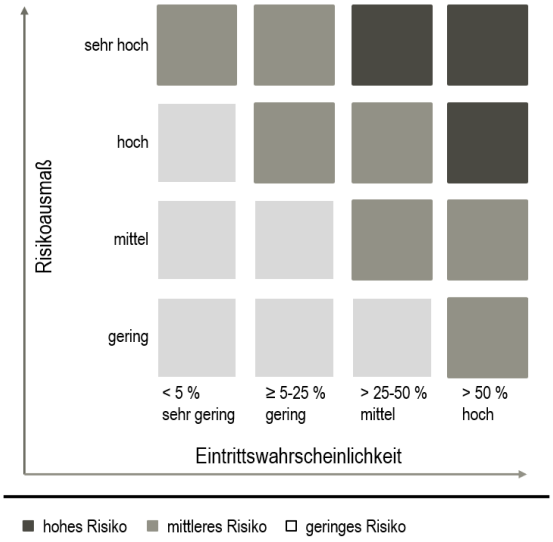
Der Aufsichtsrat sollte sich insbesondere darüber informieren lassen, wer bzw. welche Stellen im Unternehmen in den Prozess der Risikoidentifizierung eingebunden ist. Wie werden z. B. die operativ eingebundenen Mitarbeiter berücksichtigt? In Einzelfällen kann auch zu hinterfragen sein, ob und, falls ja, inwieweit sich Beurteilungen von Fachebene und Managementebene unterscheiden.

8 Wie werden Risiken bewertet?

Nach der Risikoidentifikation erfolgt die Risikobeurteilung. Diese ermöglicht es dem Unternehmen einzuschätzen, wie sich potenzielle Ereignisse auf die Zielerreichung auswirken. Das Resultat einer jeden Risikobeurteilung ist die Bewertung der Risiken im Hinblick auf Eintrittswahrscheinlichkeit und Schadenausmaß, ihre Einteilung in bestandsgefährdende und nicht bestandgefährdende sowie die Veranschaulichung des Ergebnisses in einem Risikoportfolio.

Das Risikoportfolio kann beispielsweise grafisch als Risikomatrix dargestellt werden:

Risikoportfolio als Risikomatrix



Quelle: Deutsche Telekom AG – Geschäftsbericht 2021

Hans Böckler Stiftung

Im Anschluss an die Risikobewertung müssen die Risikoklassen definiert werden, die anzeigen, welche Risiken weniger bedeutend sind und welche Risiken Steuerungsmaßnahmen erfordern. Dabei ist die Festlegung von Wesentlichkeitsgrenzen bzw. Schwellenwerten (in der Regel zu Schadenausmaß und Eintrittswahrscheinlichkeit) anhand der spezifischen Unternehmenssituation und des zur Risikoabfederung verfügbaren Eigenkapitals zu treffen.

Auch Risiken, die sich nicht oder nur schwer quantifizieren lassen (z. B. Reputationsrisiken), müssen nach Schadenausmaß und Eintrittswahrscheinlichkeit gegebenenfalls in Bandbreiten systematisiert und einer der genannten Risikoklassen zugeordnet werden.

Praxistipp:

Probleme macht in der Praxis insbesondere die Risikoaggregation. Damit sind die monetär bewerteten Wechselwirkungen von Einzelrisiken gemeint, da sich Einzelrisiken in ihrer Wirkung verstärken, aber auch kompensieren können. Der Aufsichtsrat sollte daher insbesondere kritisch hinterfragen, wie und durch wen die Risikoaggregation im Unternehmen erfolgt. Das daraus abgeleitete Gesamtrisiko wird vielfach nur in Relation zum Eigenkapital gesetzt. Es sollte darauf geachtet werden, dass es (auch) in Relation zur Liquidität gemessen und beurteilt wird, da in der Praxis eine drohende Illiquidität oft früher als eine drohende bilanzielle Überschuldung eintritt bzw. auch eine Überschuldung erst dann zur Insolvenz führt, wenn gemessen an der Liquiditätsplanung eine negative Fortführungsprognose für die kommenden zwölf Monate besteht.

9 Wie werden Risiken gesteuert?

Nach der Risikobeurteilung müssen Maßnahmen zur Risikosteuerung festgelegt werden. Mit der Risikosteuerung beginnt das aktive Risikomanagement. Gegenstand der Risikosteuerung ist es, die ermittelten und analysierten Risiken durch gezielte Maßnahmen zu steuern. Ziel ist es zum Beispiel, die auf Basis der Risikostrategie festgelegte Risikoposition einzuhalten, bei der ein ausgewogenes Verhältnis zwischen Chance/Ertrag und Risiko/Verlustpotenzial erreicht wird oder eine maximale (Netto-)Risikoposition nicht zu überschreiten.

Bestehen verschiedene Möglichkeiten, ein Risiko zu steuern, so sollte für jede Möglichkeit eine Aufwand-Nutzen-Analyse durchgeführt werden. Auszuwählen ist die Alternative, die in Bezug auf ihre Relation zwischen Nutzen und monetärem Aufwand am effizientesten ist.

Das heißt, dass für unterschiedliche Risiken auch durchaus unterschiedliche Steuerungsmaßnahmen existieren und sich die Entscheidung für eine Steuerungsmaßnahme z. B. am Kriterium der Wirtschaftlichkeit („Aufwand-Nutzen-Analyse“) orientieren kann/soll.

Allgemeine Maßnahmen der Risikosteuerung sind:

– Risikovermeidung,
– Risikoreduktion,
– Risikoteilung und schließlich auch
– Risikoakzeptanz.

Die Risikovermeidung als Steuerungsmaßnahme bietet sich bei risikobehafteten Entscheidungen an, wenn dem Unternehmensziel „Sicherheit“ gegenüber anderen Unternehmenszielen wie „Umsatz und Wachstum“ Priorität eingeräumt wird (z. B. bestimmte geografische Märkte).

Die Risikosteuerung kann auch durch Kompensation des Risikos durch ein gegenläufiges Geschäft erfolgen. Des Weiteren können Richtlinien und Risikolimits festgelegt werden, die regeln, wie Risiken zu behandeln sind und bis zu welcher Höhe Risiken eingegangen werden dürfen.

Risikoteilung findet statt, wenn Risiken auf Dritte übertragen werden. Dies ist beispielsweise durch Abschluss einer Versicherung oder Transfer auf Lieferanten oder Kunden möglich.

Die letzte Maßnahme der Risikosteuerung ist die Risikoakzeptanz, wenn die Risiken, die sich nur minimal auf das Unternehmensergebnis auswirken, zunächst ohne das Ergreifen von Steuerungsmaßnahmen akzeptiert werden können. Dennoch müssen sie von einem unternehmensweiten Überwachungssystem erfasst werden, da auch eine Kumulation minimaler Risiken mittel- bis langfristig zu einer Schwächung der Ertragssituation führen kann.

In Abhängigkeit von der Risikosteuerungsmaßnahme kann abschließend zwischen Brutto- und Nettorisiken unterschieden werden. Als Nettorisiko wird das nach Risikosteuerung verbleibende Restrisiko bezeichnet. Beispiel: Das Risiko (1.000 Geldeinheiten) kann vollständig, aber mit einem

Selbstbehalt (10 Geldeinheiten) versichert werden. Das Nettorisiko beträgt daher 10 Geldeinheiten.

Die Kenntnis von Brutto- und Nettorisiko ist wichtig, weil eine Risikobetrachtung nur auf „Netto-Ebene“ das Risiko vernachlässigen würde, dass einzelne Risikosteuerungsmaßnahmen nicht wie geplant funktionieren.

Praxistipp: Was versteht man unter Risikotragfähigkeit?

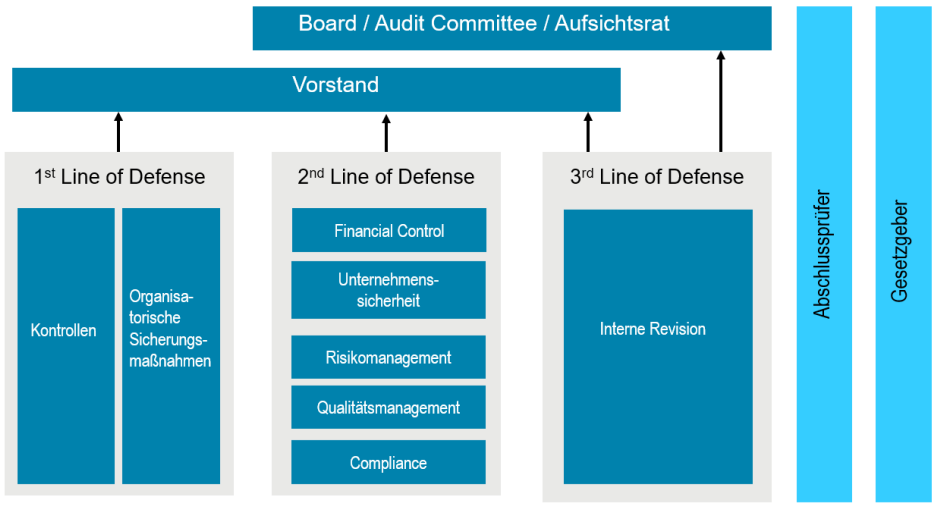
Risikotragfähigkeit ist im Sinne des IDW PS 340 n.F. das maximale Risikoausmaß, welches das Unternehmen ohne Gefährdung seines Fortbestands tragen kann. Es versteht sich also als Gegenüberstellung des Gesamtrisikos mit den zur Risikodeckung verfügbaren finanziellen Mitteln, der sogenannten Deckungsmasse. Bei der Deckungsmasse handelt es sich um betriebswirtschaftliche Größen der Vermögens-, Finanz- und Ertragslage, welche bei Risikoeintritten zur Abpufferung der Auswirkungen herangezogen werden (z. B. Eigenkapital, frei verfügbare Liquidität). Ist dabei das Verhältnis von Deckungsmasse zu Gesamtrisiko nicht ausreichend, können Unternehmen im Falle des gleichzeitigen Eintritts unterschiedlicher Risiken in eine Bestandsgefährdung geraten.
Ohne Betrachtung der Risikotragfähigkeit kann letztlich keine fundierte Aussage über die Bestandsgefährdung des Unternehmens getroffen werden, weil unklar ist, in welchem Verhältnis das Gesamtrisiko zur finanziellen Deckungsmasse steht.

10 Wie werden Kontrollaktivitäten durchgeführt?

Kontrollaktivitäten bzw. Kontrollen sind Grundsätze und Verfahren, die sicherstellen sollen, dass die Entscheidungen der Unternehmensleitung eingehalten werden. Kontrollen tragen dazu bei, dass die notwendigen Maßnahmen getroffen werden, um den Risiken des Unternehmens zu begegnen und sind in den Prozess der Risikobeurteilung integriert. Kontrollaktivitäten beinhalten in der Regel Richtlinien zur Etablierung von Soll-Vorgaben und Verfahren zur Umsetzung der Richtlinie (z. B. Vier-Augen-Prinzip).

Die verschiedenen Kontrollaktivitäten in einem Unternehmen werden in der Literatur oft durch das sogenannte Three-Lines-of-Defense-Modell beschrieben:

Three Lines of Defense Model



Quelle: Institute of Internal Auditors (IIA)

Hans Böckler Stiftung

Effiziente Information und Kommunikation

Information und Kommunikation der Risiken dienen dazu, dass die für die unternehmerischen Entscheidungen der Unternehmensleitung erforderlichen und relevanten Informationen in geeigneter Form und zeitgerecht eingeholt, aufbereitet und an die zuständigen Stellen im Unternehmen weitergeleitet werden. Dies umfasst auch die für die Risikobeurteilung notwendigen Informationen sowie die Informationen der Mitarbeiter über Aufgaben und Verantwortlichkeiten im RMS. Neben der mündlichen Berichterstattung können Organisationshandbücher, Richtlinien für die interne und externe Rechnungslegung, Aktennotizen und ähnliches in Betracht kommen.

Relevante Informationen aus internen und externen Quellen müssen in einer Form und einem zeitlichen Rahmen identifiziert, dokumentiert und kommuniziert werden, die es der Unternehmensleitung und den Mitarbeitern ermöglichen, ihre jeweiligen Verantwortlichkeiten zu erfüllen.

Für die effektive Kommunikation innerhalb eines Unternehmens müssen offene und eindeutige Kommunikationswege bestehen („Berichtslinien“). Die Unternehmensleitung hat für die notwendigen Kommunikationswege zu sorgen. Dies mindert die Gefahr, dass die Unternehmensleitung zu spät von den Risiken erfährt. Ebenso muss die Kommunikation zwischen Unternehmensleitung und Aufsichtsrat sichergestellt sein, um die notwendige Informationsversorgung beider Parteien zu gewährleisten.

Praxistipp:

Das RMS darf nicht isoliert betrachtet, sondern sollte als integraler Bestandteil der Unternehmensorganisation verstanden werden. Der Aufsichtsrat sollte besonders darauf achten, dass Informationen aus dem

RMS auch in anderen Zusammenhängen, z. B. bei Beschlussvorlagen zu zustimmungspflichtigen Geschäften (Investitionsentscheidungen …), berücksichtigt werden. Bezogen auf Investitionsentscheidungen, können das beispielsweise Risikoanalysen sein, in denen die mit der Investition verbundenen Risiken bewertet und beurteilt werden können. In der Regel werden in Risikoanalysen, insbesondere bei wesentlichen Investitionsentscheidungen, verschiedene Szenarien (z. B. Kostenentwicklung bei mehrjährigen Bauvorhaben oder Umsatzerlösentwicklung) durchgerechnet.

Berichtsordnung und -turnus

Die strukturierte und systematisierte Kommunikation von Risiken muss durch die Risikoberichterstattung sichergestellt werden. Die Risikoberichterstattung setzt die organisatorische Einbindung des Risikomanagements im gesamten Managementprozess voraus. Unternehmensleitung, Interne Revision, Aufsichtsrat, Abschlussprüfer, (Risiko-)Controlling und Mitarbeiter sind in eine formale interne Risikoberichterstattung einzubeziehen und aufbau- und ablauforganisatorisch aufeinander abzustimmen.

Überwachung der identifizierten Risiken

Die Überwachung der identifizierten Risiken erfolgt im gesamten Unternehmen, z. B. auf den Hierarchieebenen der Unternehmensleitung, des Aufsichtsrats, der Internen Revision sowie des operativen Managements. Die Überwachung muss sicherstellen, dass das RMS funktionsfähig ist und kontinuierlich auf allen Ebenen im gesamten Unternehmen angewendet wird.

Die Überwachung soll die Wirksamkeit des RMS durch die Mitarbeiter des Unternehmens sicherstellen. Die Unternehmensleitung hat zusätzlich dafür zu sorgen, dass festgestellte Mängel im RMS in geeigneter und zeitnaher Weise behoben werden. Das RMS wird auch von der Internen Revision überwacht. Zu den Aufgaben der Internen Revision zählt unter anderem die Entwicklung von Verbesserungsvorschlägen für die Wirksamkeit des RMS.

Das RMS soll kontinuierlich beurteilt werden. Laufende Beurteilungen sind beispielsweise durch die regelmäßige Durchsicht von Berichten durch die Unternehmensleitung sowie durch den Vergleich von Ist-Zahlen zu Plan- und Budget-Zahlen durchzuführen. Gesonderte Beurteilungen werden durch die Unternehmensleitung, die Interne Revision, externe Spezialisten oder eine Kombination der drei Gruppen durchgeführt.

Zur Sicherstellung der dauerhaften Funktionsfähigkeit des Risikomanagementprozesses sowie zum Nachweis der Erfüllung der Organisations- und Sorgfaltspflichten der Unternehmensleitung ist eine ordnungsgemäße und zeitnahe Dokumentation erforderlich. Diese umfasst neben der Dokumentation der getroffenen Entscheidungen auch die Beschreibung des gesamten RMS in einem Handbuch bzw. einer Richtlinie. Die Beschreibung des RMS gibt den Mitarbeitern Verhaltensnormen und Verhaltensanweisungen bzgl.

der Risiken vor und dient als Grundlage für die Prüfung des Systems durch den Aufsichtsrat, die Interne Revision und den Abschlussprüfer.

11 Aufgaben zentraler Unternehmensorgane

Der Aufsichtsrat hat die Wirksamkeit des RMS, das durch den Vorstand zu implementieren ist, zu überwachen. Bei dieser Überwachung wird der Aufsichtsrat sowohl durch die Interne Revision als auch durch den Abschlussprüfer unterstützt. Der Aufsichtsrat sollte daher insbesondere auf Erkenntnisse dieser Gruppen zurückgreifen.

Prüfungsausschuss bzw. Aufsichtsrat

Nach § 107 Abs. 3 AktG sollte der Aufsichtsrat einen Prüfungsausschuss bestellen, der sich mit der Überwachung des RMS befasst. Sofern kein Prüfungsausschuss eingerichtet ist, muss der Gesamtaufsichtsrat diese Verantwortung wahrnehmen.

Der Aufsichtsrat bzw. Prüfungsausschuss ist verpflichtet, die Wirksamkeit des RMS zu beurteilen. Die Beurteilung der Wirksamkeit muss mit hinreichender Sicherheit ergeben, dass das RMS auch tatsächlich wirksam ist, wobei die Unternehmensleitung zuvor diese Wirksamkeit sicherzustellen hat. Der Aufsichtsrat hat sich über die durch die Unternehmensleitung ergriffenen Maßnahmen sowie die Ergebnisse der Prüfungen informieren zu lassen. Bei Zweifeln an der ihm mitgeteilten Einschätzung muss der Aufsichtsrat eigene Untersuchungen beauftragen und im Falle der Identifizierung von Optimierungsbedarf auf die Verbesserung des RMS hinwirken und diesen Prozess überwachen.

Spezielle Aufgaben der Mitglieder des Prüfungsausschusses oder des gesamten Aufsichtsrats sind:

– kritisches Hinterfragen der Aktivitäten der Geschäftsleitung (z. B. liegt eine Risikoanalyse bei zustimmungspflichtigen Investitionsentscheidungen vor?),
– Begleitung der Geschäftsleitung als Berater bei der kontinuierlichen Weiterentwicklung von RMS entsprechend den strategischen Vorgaben.

Interne Revision

Die Interne Revision übt einerseits eine übergeordnete prozessunabhängige Kontrollfunktion im Hinblick auf das RMS aus. Das RMS ist also selbst Prüfungsgegenstand der Internen Revision. Andererseits umfassen auch die Prüfungstätigkeiten der Internen Revision im Rahmen anderer Prüfungen regelmäßig Aspekte des RMS. Prüft die Interne Revision beispielsweise kaufmännische Prozesse, prüft sie auch, ob z. B. Risikoanalysen im Rahmen von Investitionsentscheidungen erstellt und berücksichtigt worden sind.

Abschlussprüfer*innen

Im Rahmen der gesetzlichen Jahresabschlussprüfung stehen naheliegend der Jahresabschluss (Bilanz, Gewinn- und Verlustrechnung und Anhang) sowie gegebenenfalls der Lagebericht im Fokus des Abschlussprüfers. Darüber hinaus sind Gegenstand der Prüfung die Buchführung, das interne Kontrollsystem und im Fall von börsennotierten Unternehmen auch das Risikofrüherkennungssystem (§ 317 Abs. 4 HGB).

Allerdings sind nur die rechnungslegungsbezogenen Bestandteile des internen Kontrollsystems und des Risikomanagementsystems Teil der Prüfung durch den Abschlussprüfer. Der Prüfungsauftrag nach § 317 HGB umfasst nicht die Prüfung und Beurteilung der Risikosteuerung, d. h. der Beurteilung der Wirksamkeit und Wirtschaftlichkeit der getroffenen Maßnahmen. Der Abschlussprüfer beschränkt sich auf die Prüfung des Risikofrüherkennungssystems gemäß § 91 Abs. 2 AktG.

Abgrenzend zur gesetzlichen Pflichtprüfung durch den Wirtschaftsprüfer, die vorstehend dargestellt ist, besteht die Möglichkeit zur freiwilligen Prüfung des (gesamten) Risikomanagementsystems durch einen Wirtschaftsprüfer nach IDW PS 981.

Der Aufsichtsrat kann die Wirksamkeit des RMS also nicht (ausschließlich) auf Basis des Urteils des Abschlussprüfers im Rahmen der Jahresabschlussprüfung beurteilen, weil Gegenstand der Prüfung durch den Abschlussprüfer nicht das gesamte RMS, sondern nur das Risikofrüherkennungssystem ist.

12 Wie kann der Aufsichtsrat die Wirksamkeit des RMS beurteilen?

Bei der Beurteilung der Wirksamkeit des RMS ist der Aufsichtsrat auf die Information über die Risikolage und den Aufbau des RMS angewiesen. Grundlage für die Informationsbeschaffung ist die Dokumentation des RMS, aus der die Risiken sowie die zugrunde liegenden Prozesse und Ergebnisse der Wirksamkeitsprüfung hervorgehen.

Die Unternehmensleitung hat sämtliche Informationen über die wesentlichen Instrumente des RMS sowie die Auskunft über Ergebnisse aus der Analyse der Angemessenheit und Funktionsfähigkeit des RMS bereitzustellen. Zudem hat der Vorstand über die festgestellten Schwächen bzw. Verstöße sowie über den Status der Beseitigung wesentlicher Schwächen und den Umsetzungsstand von Aufträgen des Aufsichtsrats zu berichten.

Des Weiteren kann eine „Erklärung“ der Unternehmensleitung die Grundlage für die Beurteilung des RMS darstellen. In der jährlichen „Erklärung“ kann die Unternehmensleitung die Angemessenheit und Wirksamkeit des RMS beurteilen und Fehler, Manipulationen sowie wesentliche Änderungen des RMS nach Jahresende bekannt geben.

Die Hinzuziehung von Sachverständigen und Auskunftspersonen zu den Sitzungen des Aufsichtsrats ist eine Möglichkeit, die Informationslage zur

Wirksamkeit des RMS zu verbessern. Insbesondere stellen die Berichte der Internen Revision eine wesentliche Unterstützung dar, um die Wirksamkeit des RMS beurteilen zu können.

Praxistipp:

Damit der Aufsichtsrat die Wirksamkeit des RMS beurteilen kann, braucht er angemessene Informationen. Der Vorstand einer AG unterliegt zwar bestimmten Berichtspflichten (§ 90 Abs. 1 AktG), aber das heißt nicht, dass der Aufsichtsrat nicht selbst Informationen anfordern muss, wenn er sich nicht angemessen informiert fühlt („Information ist auch Holschuld"). Entspricht die interne Risikoberichterstattung nicht den Erwartungen des Aufsichtsrats (Umfang und/oder Inhalt), muss er auf eine Verbesserung hinwirken.
Insbesondere über § 91 Abs. 3 AktG ist die Möglichkeit auch für jedes einzelne Mitglied des Aufsichtsrats eröffnet, zusätzliche Informationen beim Vorstand anzufordern. Dieses Recht gilt auch für den „GmbH-Aufsichtsrat" gemäß § 52 Abs. 1 GmbHG.

12.1 Anforderungen an die Berichterstattung

Für eine wirksame Überwachung ist eine periodische Berichterstattung über die Risikolage und den Aufbau des RMS durch die Geschäftsleitung an den Aufsichtsrat notwendig. Je nach den spezifischen Rahmenbedingungen des Unternehmens kann diese Berichterstattung einige wenige Leistungskennzahlen (KPIs) umfassen oder aus einem voll integrierten, automatisierten Berichtssystem bestehen.

Die Berichterstattung hat in regelmäßigen Abständen zu erfolgen. Dabei werden die von der Planung aufgestellten Planvorhaben (Sollstand) regelmäßig mit den tatsächlich erreichten Werten (Iststand) verglichen. Im Rahmen der Beurteilung werden die Abweichungen analysiert und ggf. daraus resultierende notwendige Maßnahmen eingeleitet, um die Lücken zum Sollstand zu schließen.

Praxistipp:

Häufig ist zu beobachten, dass Unternehmen über Risiken, die in der Planung berücksichtigt worden sind (z. B. durch Rückstellungsbildung oder durch angepasste Umsatzerlöse und/oder Aufwendungen), nicht mehr berichten. Begründet wird dieses Vorgehen damit, dass ein Risiko per Definition eine Planabweichung darstellt. Wenn das Risiko aber bereits in der Planung berücksichtigt ist, kann es nach dieser Logik nicht mehr zu Planabweichungen führen. Der Aufsichtsrat muss zunächst nachvollziehen, wie das von ihm überwachte Unternehmen mit Risiken, deren Auswirkungen bereits vollständig planerisch berücksichtigt worden sind, umgeht. Falls über diese Risiken nicht mehr im Rahmen der Risikoberichterstattung berichtet wird und sie noch nicht eingetreten sind, muss der Aufsichtsrat ggfs. auf eine Änderung hinwirken.

12.2 Self-Assessment

Das Self-Assessment („Selbsteinschätzung“) stellt eine Methode zur Identifikation und Messung der Wirksamkeit des RMS dar. Die einzelnen Unternehmensbereiche sollten regelmäßig selbst anhand eines Fragebogens die Verlässlichkeit und den Reifegrad des jeweils für den Teilbereich relevanten RMS einschätzen.

Periodische unternehmensinterne Selbsteinschätzungen des RMS lassen Rückschlüsse auf Effektivität, Nachhaltigkeit und Reifegrad des gelebten RMS zu.

12.3 Ergebnisse der Abschlussprüfung

Der Abschlussprüfer hat die von ihm identifizierten Risiken und Schwächen im RMS zu kommunizieren. Zudem sollte der Aufsichtsrat den Abschlussprüfer zu seiner Einschätzung des RMS und zu Verbesserungsvorschlägen befragen, selbst wenn keine wesentlichen Schwächen festgestellt wurden.

Hinweis:

Die Prüfung des Risikofrüherkennungssystems durch den Abschlussprüfer nach § 317 Abs. 4 in Verbindung mit § 91 Abs. 2 AktG bedeutet nicht, dass das RMS insgesamt wirksam ist oder nicht. Allgemeine festgestellte Mängel des Risikofrüherkennungssystems führen nicht zur Einschränkung des Bestätigungsvermerks des Abschlussprüfers.
Der Aufsichtsrat sollte den Abschlussprüfer als Ansprechpartner in allen Fragen rund um das RMS nutzen, um über die für die Finanzberichterstattung relevanten Risiken informiert zu sein, deren Beurteilung für die Erlangung eines Prüfungsurteils notwendig ist.
Risiken und interne Kontrollen hinsichtlich strategischer, operationeller und Compliance-bezogener Ziele sind nicht Gegenstand einer Abschlussprüfung. Da der Abschlussprüfer aber häufig fundiertes Prozess- und Risikowissen über die Finanzberichterstattung hinaus besitzt, kann er über gesonderte Aufträge in den genannten Bereichen wertvolle Analysen durchführen.

12.4 Kritisches Hinterfragen der Unternehmensleitung

Damit der Aufsichtsrat das RMS angemessen überwachen kann, sollte er stets die Einschätzung der Risiken seitens der Unternehmensleitung kritisch hinterfragen und Risikoinformationen diskutieren.

In bestimmten Fragen von besonderer Bedeutung – insbesondere dann, wenn sich der Aufsichtsrat sonst kein umfassendes Bild verschaffen kann – ist auch die direkte Befragung bestimmter Mitarbeiter in Stabsfunktionen (z. B. aus den Bereichen Finanzwesen, Compliance, Interne Revision, Recht, Steuern oder IT) oder aus der Linie (z. B. Leiter Produktion, Einkauf oder Verkauf wesentlicher Tochtergesellschaften) möglich. Ein

„Direktauskunftsrecht“ des Prüfungsausschusses bzw. des Ausschussvorsitzenden gegenüber den Leitern der Unternehmensfunktionen, die der Prüfungsausschuss zu überwachen hat (z. B. RMS), hat der Gesetzgeber mit Umsetzung des FISG (vgl. Karteikarte 1) auch in § 107 Abs. 4 S. 4 AktG legal definiert. Dieses Auskunftsrecht wirkt unmittelbar. Der Vorstand ist über ein solches Auskunftsersuchen lediglich zu informieren.

13 Links und Literatur

Eulerich, Marc (2017): ➔I Risikomanagement im Aufsichtsrat: Ein Handbuch für Arbeitnehmervertreter im Aufsichtsrat, MB Praxis 07/2017, Hans-Böckler-Stiftung

Eisbach, Joachim (2015): ➔I Der Risikobericht als Bestandteil des Lageberichts, Edition der Hans-Böckler-Stiftung Nr. 295

Steinhaus, Henrik / Guttzeit, Mandy (2021): ➔I Management unternehmensstrategischer Risiken – Früherkennung von Indikatoren für Beschäftigungsrisiken, MB Praxis 42/2021, Hans-Böckler-Stiftung

Gossens, Thomas / Wendt, Mathias (2018): ➔I Die Zusammenarbeit zwischen Interner Revision und Aufsichtsrat, Arbeitshilfe für Aufsichtsräte Nr. 19, Hans-Böckler-Stiftung

Ansprechpartner in der Hans-Böckler-Stiftung

Alexander Sekanina

Über den Autor

Lars Beermann ist Wirtschaftsprüfer, Steuerberater und Partner der Korthäuer & Partner GmbH, Wirtschaftsprüfungsgesellschaft, Steuerberatungsgesellschaft, Essen, und dort unter anderem tätig in den Bereichen der betriebswirtschaftlichen Prüfungen und Beratungen. Ein Schwerpunkt seiner Tätigkeiten liegt in der betriebswirtschaftlichen Qualifizierung von Betriebsräten, Wirtschaftsausschüssen und Arbeitnehmervertreter*innen in Aufsichtsräten.

Kontakt

Impressum

Erschienen im Mitbestimmungsportal, dem Infoservice der Hans-Böckler-Stiftung für die Mitbestimmungspraxis. Die Reihe "Wissen kompakt" bietet im Kartenstapel-Format anschaulich und komprimiert aufbereitete Hintergrundinformationen zu aktuellen Themen.

Online-Fassung und weitere Themen unter www.mitbestimmung.de/wissen-kompakt

Kontakt:
Michael Stollt
Hans-Böckler-Stiftung
Georg-Glock-Straße 18
40474 Düsseldorf
mitbestimmungsportal@boeckler.de

Hans-Böckler-Stiftung,
August 2022