DIIR Revisionsstandard Nr. 2: Prüfung des Risiko-managementsystems durch die Interne Revision

Version 2.0

DIIR Deutsches Institut für Interne Revision e.V.

Inhalt

1 Präambel

1 Das Risikomanagement ist Führungsaufgabe und integraler Bestandteil aller Geschäftsprozesse inklusive der Planungs- und Überwachungsprozesse jeder Organisation. Der Prüfung des Risikomanagementsystems kommt damit eine besondere Bedeutung zu.

2 Die Interne Revision ist neben anderen Funktionen in einer Organisation, wie Compliance, Risikomanagement und Controlling, Bestandteil des internen Überwachungssystems. Gemäß dem Three Lines of Defense-Modell hat die Interne Revision als Third Line neben der First Line auch die Prozesse der Funktionen in der Second Line (z. B. Compliance, Risikomanagement, Controlling, Qualitätsmanagement) in ihre Prüfungstätigkeiten einzubeziehen.

3 Ziel dieses Standards ist die Darstellung von Grundsätzen für die Prüfung des Risikomanagementsystems durch die Interne Revision. Dieser Standard bildet ein Rahmenwerk zur Planung und Durchführung von Prüfungen des Risikomanagementsystems und ist auch für kleinere Organisationen anwendbar. Er stellt bewusst keinen konkreten Prüfungsplan dar. Ergänzend werden durch das DIIR Hinweise zur Prüfung, z. B. in Form von Checklisten, veröffentlicht.

4 Zur Konkretisierung eines Prüfungsplans sind die in diesem Standard dargestellten Grundsätze anhand der jeweiligen organisationsspezifischen Gegebenheiten risikoorientiert in einzelne Prüfungsgebiete und -handlungen umzusetzen. Dabei wird das Einbeziehen von Risikomanagementstandards, z. B. COSO ERM Integrated Framework oder ISO 31000, empfohlen.

5 Die Prüfung muss auch die gesetzlichen Anforderungen aus § 91 (2) und § 107 (3) AktG berücksichtigen, insbesondere die frühe Erkennung bestandsgefährdender Entwicklungen, die sich meist aus Kombinationseffekten mehrerer Einzelrisiken ergeben. Prüfungsgegenstand ist das gesamte Überwachungssystem, d. h. das Risikomanagementsystem im weiteren Sinn, das alle Managementsysteme umfasst, die sich mit Risiken befassen. Aufgrund der Ausstrahlungswirkung gelten diese Anforderungen sinngemäß auch für große Unternehmen im Sinne des § 267 Abs. 3 HGB, kapitalmarktorientierte Unternehmen und öffentliche Unternehmen.

6 Dieser Standard ersetzt nicht die weitaus detaillierteren Ansätze zur Prüfung des Risikomanagementsystems in Branchen, in denen die externen Regelungen zur Risikomanagementfunktion und deren Umsetzung seit vielen Jahren ein wesentliches Prüffeld der Internen Revision sind.

2 Adressaten, Geltungsbereich und Verbindlichkeit des Standards

7 Der vorliegende Standard richtet sich vorrangig an Leiter und Mitarbeiter von Internen Revisionseinheiten. Darüber hinaus unterstützt er durch die definierten Anforderungen an die Prüfung eines Risikomanagementsystems Vorstände und Aufsichtsräte bei der Erfüllung ihrer Sorgfalts- und Überwachungspflichten sowie Abschlussprüfer in Bezug auf die Zusammenarbeit mit der Internen Revision. Verantwortlichen in den Bereichen Risikomanagement, Compliance und Controlling geben die vorgegebenen Prüfungsinhalte ein klareres Bild der Anforderungen an ein Risikomanagementsystem.

8 Dieser Revisionsstandard wurde vom DIIR – Deutsches Institut für Interne Revision e.V. in einem sorgfältigen Verfahren entwickelt und verabschiedet. Er ergänzt als lokale Leitlinie das International Professional Practice Framework (IPPF). Die Anwendung dieses Revisionsstandards wird für Interne Revisoren in Deutschland dringend empfohlen.

3 Rechtliche Grundlagen des Risikomanagementsystems

9 Rechtliche Grundlagen, aus denen sich Anforderungen zur Einrichtung eines Risikomanagementsystems und dessen Überwachungspflicht direkt oder indirekt ableiten lassen, existieren in vielfältiger Form und variieren insbesondere je nach Branche und Rechtsform der Organisation. Sie ergeben sich aus allgemeinen gesetzlichen Regelungen (bspw. Handelsrecht und Aktiengesetz) und auch aus branchenspezifischen Regelungen (bspw. Finanzbranche (MaRisk)).

10 Während im Handelsrecht (§§ 289 und 315 HGB) die Berichtspflichten über das Risikomanagementsystem im Lagebericht beschrieben werden, fordert insbesondere das Aktiengesetz in § 91 Abs. 2 vom Vorstand die Einrichtung eines Überwachungssystems, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden. In der Gesetzesbegründung präzisiert der Gesetzgeber diese Anforderung mit der Verpflichtung des Vorstands, für ein angemessenes Risikomanagement zu sorgen. Im Jahr 2009 wurden mit dem Bilanzrechtsmodernisierungsgesetz (BilMoG) zudem die Überwachungspflichten des Aufsichtsrats im Hinblick auf das unternehmensweite Risikomanagementsystem in § 107 Abs. 3 AktG konkretisiert. Die Regelungen des Aktiengesetzes haben für Organisationen anderer Rechtsformen je nach Größe, Komplexität und Struktur eine Ausstrahlungswirkung.

11 Für die Finanzbranche wurden durch die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) Grundsätze für die Ausgestaltung des Risikomanagements sowie spezifische Anforderungen an die Organisation und die Prozesse für das Management und Controlling von Adressenausfall-, Marktpreis-, Liquiditäts- sowie operationellen Risiken festgelegt. Außerdem wurde dort ein Rahmen für die Ausgestaltung der Internen Revision vorgegeben.

12 Für die öffentlichen Bereiche kann die Verpflichtung zu einem Risikomanagement aus § 53 des Haushaltsgrundsätzegesetzes sowie aus der Bundeshaushaltsordnung, den Landeshaushaltsordnungen und den Gemeindeordnungen der jeweiligen Länder abgeleitet werden.

13 Darüber hinaus ist der Deutsche Rechnungslegungsstandard DRS 20 (Konzernlagebericht) zu beachten, der Regelungen zur Risikoberichterstattung enthält.

4 Begriffsdefinitionen

14 Dieser Standard verwendet nachfolgende Definitionen. Eine Vielzahl von Normen, Standards und anderen Veröffentlichungen verwendet diese Begriffe in ähnlicher, oft aber enger oder weiter gefasster Weise. Jede Organisation muss für sich im Kontext der jeweiligen Betrachtung festlegen, welche die für sie geeigneten Definitionen sind.

15 Risiko

Der Begriff Risiko beschreibt die Möglichkeit des Eintretens von Ereignissen oder von Entwicklungen, die sich auf das Erreichen von Zielen auswirken, was die Möglichkeit von positiven Abweichungen (Chancen) und negativen Abweichungen (Gefahren, Risiken im engeren Sinn) einschließt. Die Analyse und Quantifizierung von Risiken setzt damit grundsätzlich die Transparenz über die zugrundeliegenden Ziele voraus. Ein Risiko entsteht infolge der bestehenden Unsicherheiten oder der unvollständigen Informationen in Bezug auf die zukünftige Entwicklung von Zielgrößen. Exemplarische Risikokategorien sind strategische Risiken, Marktrisiken, operative Risiken, Berichterstattungs- sowie Compliancerisiken.

16 Risikomanagement

Risikomanagement bezeichnet alle Tätigkeiten, die darauf ausgerichtet sind, Risiken frühzeitig und systematisch zu erfassen, zu steuern und zu überwachen. Es gehört auch zu den Aufgaben des Risikomanagements sicherzustellen, dass schon bei der Vorbereitung wesentlicher unternehmerischer Entscheidungen deren Implikationen für den zukünftigen Risikoumfang nachvollziehbar aufgezeigt werden, um zumindest eine mit solchen Entscheidungen möglicherweise einhergehende bestandsgefährdende Entwicklung früh zu erkennen. Neben bereits vorhandenen Risiken sind damit durch das Risikomanagement insbesondere auch geplante Maßnahmen und Entscheidungen zu betrachten, speziell im Hinblick auf durch diese möglicherweise verursachten zukünftigen Risiken. Die alleinige Überwachung schon identifizierter Risiken ist unzureichend. Dies umfasst die nachvollziehbare und regelmäßige Identifikation von Risiken, deren Analyse und Bewertung, die Implementierung geeigneter Risikosteuerungsmaßnahmen und deren Kontrolle sowie die regelmäßige Berichterstattung und die fortlaufende Überwachung der Risiken und der zuvor genannten Prozessschritte.

17 Risikomanagementsystem

Ein Risikomanagementsystem ist der von der Leitung der Organisation vorgegebene aufbau- und ablauforganisatorische Rahmen zur Umsetzung des Risikomanagements. Ausgangspunkt eines Risikomanagementsystems ist die Festlegung von Rahmenbedingungen durch die Geschäftsleitung, wie Organisationsziele, Risikopolitik, Verhaltensregeln, Verant-

wortlichkeiten und Kompetenzen, in denen die Geschäftsprozesse inklusive der Risikomanagementtätigkeiten ablaufen. Dies kann strategische Planung, Entscheidungs-prozesse und andere Prozesse, die sich mit Risiken beschäftigen, beinhalten. Das Risikomanagementsystem ist regelmäßig weiterzuentwickeln und zu überwachen.

18 Angemessenheit und Wirksamkeit des Risikomanagementsystems

Ein angemessenes Risikomanagementsystem basiert insbesondere auf der Festlegung von Risikomanagementstrategien und der Einrichtung geeigneter Maßnahmen und interner Kontrollen. Wirksam ist ein Risikomanagementsystem, wenn es so ausgestaltet und in der Organisation umgesetzt ist, dass die in Abschnitt 6 beschriebenen Risikomanagementphasen aufeinander aufbauend und ordnungsgemäß durchlaufen werden, sodass die Erreichung der unternehmerischen Ziele mit ausreichender Wahrscheinlichkeit sichergestellt wird und mögliche, die Organisation beeinflussende Ereignisse erkannt werden können und darauf angemessen reagiert werden kann.

19 Risikoaggregation

Risikoaggregation ist die Methode zur Bestimmung des Gesamtrisikoumfangs, der sich aus quantifizierten Einzelrisiken unter Beachtung möglicher Kombinationseffekte und stochastischer Abhängigkeiten (wie Korrelationen) ergibt. Im Risikomanagement ist die Risikoaggregation der Risikoanalyse nachgelagert und erforderlich, um mögliche bestandsgefährdende Entwicklungen (§ 91 (2) AktG) zu erkennen, die sich im Allgemeinen aus Kombinationseffekten von Einzelrisiken ergeben.

20 Die Risikoaggregation erlaubt die Berechnung von Kennzahlen für den Gesamtrisikoumfang (Value-at-Risk oder Eigenkapitalbedarf) und daraus ableitbaren Größen (wie Insolvenzwahrscheinlichkeit oder risikogerechte Kapitalkosten). Einzelrisiken sind nicht addierbar und insbesondere durch die Monte-Carlo-Simulation ist es möglich, unterschiedliche Risikotypen (beschrieben durch unterschiedliche Wahrscheinlichkeitsverteilungen) bezogen auf die Unternehmensplanung zu aggregieren.

21 Risikodeckungspotenzial, Gesamtrisikoumfang, Risikotragfähigkeit und Risikotoleranz

Es empfiehlt sich, Kennzahlen zu definieren, die den Gesamtrisikoumfang in Relation bringen zum Risikodeckungspotenzial des Unternehmens. Entsprechend der möglichen Ursachen für bestandsgefährdende Entwicklungen und Insolvenz ist das Risikodeckungspotenzial gegeben durch a) Eigenkapital zur Abdeckung möglicher Verluste und b) Liquiditätsreserven (inkl. freier und möglicher zusätzlicher Kreditlinien) zur Abdeckung risikobedingter Liquiditätsabflüsse.

22 Beispielsweise können Kennzahlen für die Risikotragfähigkeit angegeben werden, die den Abstand des Status quo zu dem Punkt, der als bestandsgefährdende Entwicklung angesehen werden muss, und die Wahrscheinlichkeit, dass eine solche bestandsgefährdende Entwicklung auftritt, zeigen.

23 Während sich die Risikotragfähigkeit damit auf eine bestandsgefährdende Entwicklung bezieht, stellt die Risikotoleranz auf ein anspruchsvolleres, von der Unternehmensführung festgelegtes Sicherheitsziel ab.

24 Bestandsgefährdende Entwicklung

Von einer bestandsgefährdenden Entwicklung spricht man, wenn eine Situation der Überschuldung oder Zahlungsunfähigkeit droht. Letztere droht, wenn Kreditvereinbarungen (Covenants) verletzt werden, die eine Kündigung von Krediten nach sich ziehen und/oder Mindestanforderungen der Fremdkapitalgeber an das Rating nicht mehr erfüllt sind.

5 Auftrag der Internen Revision zur Prüfung des Risikomanagementsystems

25 Zu einer erfolgreichen und wertorientierten Führung einer Organisation im Sinne einer guten Corporate Governance gehört ein auf die Risikolage fokussierendes Überwachungssystem. Neben der Überwachung vorhandener Risiken ist das System der Vorbereitung von Managemententscheidungen einzubeziehen, um die Auswirkungen von Entscheidungen auf die Risikolage zu erfassen.

26 Die sich daraus ergebende Aufgabe der Internen Revision, das Risikomanagement umfassend zu prüfen, spiegelt sich in der Definition des DIIR und des Institute of Internal Auditors (IIA) wider:

> *„Die Interne Revision erbringt unabhängige und objektive Prüfungs- und Beratungsdienstleistungen, welche darauf ausgerichtet sind, Mehrwerte zu schaffen und die Geschäftsprozesse zu verbessern. Sie unterstützt die Organisation bei der Erreichung ihrer Ziele, indem Sie mit einem systematischen und zielgerichteten Ansatz die Effektivität des Risikomanagements, der Kontrollen und der Führungs- und Überwachungsprozesse bewertet und diese verbessern hilft.“*

27 Die Internationalen Standards für die berufliche Praxis der Internen Revision definieren mit dem Ausführungsstandard 2120 die Aufgabe der Internen Revision bzgl. der Prüfung des Risikomanagements:

> *„Die Interne Revision muss die Funktionsfähigkeit der Risikomanagementprozesse beurteilen und zu deren Verbesserung beitragen.“*

28 Die Erläuterung des IIA zu Standard 2120 besagt:

> *„Die Feststellung, ob Risikomanagementprozesse funktionsfähig sind, wird anhand der Beurteilung des Internen Revisors getroffen, dass:*
>
> - *die Ziele der Organisation mit deren Mission im Einklang stehen und diese unterstützen,*
> - *wesentliche Risiken erkannt und bewertet sind,*
> - *angemessene Risikomaßnahmen ergriffen worden sind, die mit der Risikoakzeptanz der Organisation im Einklang stehen und*
> - *wesentliche risikobezogene Informationen erfasst und rechtzeitig in der Organisation kommuniziert werden, sodass es Mitarbeitern, Führungskräften, und Geschäftsleitung bzw. Überwachungsorgan möglich ist, ihren Verantwortlichkeiten gerecht zu werden.“*

29 Im Zusammenhang mit der Prüfung des Risikomanagementsystems ergeben sich Prüfungserfordernisse, die sowohl die Abschlussprüfer als auch die Interne Revision betreffen. Dabei ist eine Zusammenarbeit zwischen Interner Revision und Abschlussprüfern ausdrücklich gewünscht.

6 Prüfung des Risikomanagementsystems und seiner Phasen

30 Die Funktionen des Risikomanagements lassen sich in einem Phasenmodell veranschaulichen. Ausgehend von der auf der Gesamtstrategie der Organisation aufbauenden Risikostrategie folgen auf die Identifikation und Erfassung der Risiken und deren Analyse und Bewertung die Steuerung und Überwachung mit einer Rückkopplung zur Risikostrategie und ggf. deren Anpassung. Integraler Bestandteil aller Phasen ist deren Dokumentation und die Berichterstattung bzw. Kommunikation. Abbildung 1 veranschaulicht dieses Modell.

Abb. 1: Phasenmodell des Risikomanagements

31 Die Prüfung des Risikomanagementsystems orientiert sich an den genannten Phasen und Elementen, die in den weiteren Abschnitten detaillierter ausgeführt sind. Um eine Aussage über die Angemessenheit und die Wirksamkeit des Systems treffen zu können, sind

das Design des Systems, seine Implementierung und die Wirksamkeit über einen zu definierenden Prüfungszeitraum zu prüfen.

32 Durch die Prüfung des Systemaufbaus und der festgelegten Abläufe lässt sich ein Urteil über die Angemessenheit im Sinne der Zielsetzung gewinnen. Um die Eignung des Risikomanagementsystems sowohl im Aufbau als auch in der Umsetzung beurteilen zu können, sind folgende Elemente zu betrachten: Methodik, Organisation, Aufgabenzuordnung, Prozesse, genutzte Informationssysteme einschließlich der Speicherung und Übertragung von Daten, Dokumentation, Anpassungsfähigkeit (Dynamik) und Integration in bestehende Überwachungs- und Führungssysteme.

33 Die Prüfung der betriebswirtschaftlichen Methoden betrachtet die im Risikomanagement genutzten Verfahren im Hinblick auf die Angemessenheit zur Erfüllung der gesetzten Ziele. Geprüft werden müssen dabei insbesondere die Eignung der Methoden der Risikoidentifikation, die Eignung der genutzten quantitativen Verfahren zur Beschreibung von Risiken (Wahrscheinlichkeitsverteilungen, stochastische Prozesse) und die Methoden der Risikoaggregation, speziell auch im Hinblick auf die Eignung, bestandsgefährdende Entwicklungen aus den Kombinationseffekten von Einzelrisiken zu erkennen. Ebenso zu prüfen sind die Methoden zur Berücksichtigung von Risikoinformationen bei der Entscheidungsvorbereitung.

34 Durch die Prüfung der Wirksamkeit soll festgestellt werden, ob das System tatsächlich während des gesamten Prüfungszeitraums die beabsichtigten Ergebnisse erzielt hat. Anhand konkreter Fälle ist zu prüfen, ob die Vorgaben eingehalten wurden und die getroffenen Aussagen belastbar sind.

6.1 Risikomanagement-Organisation und Risikokultur

35 Aufbauorganisation

Die Verantwortung für das Risikomanagementsystem ist in der Geschäftsleitung verankert. Als Gesamt- und damit auch Risikoverantwortliche ist die Geschäftsleitung speziell im Rahmen der Definition der Risikostrategie und der Rahmenvorgaben für die Implementierung geeigneter Steuerungsmaßnahmen Bestandteil des Risikomanagementsystems. Darüber hinaus ist die Geschäftsleitung dafür verantwortlich, dass die Funktionen des Risikomanagements wirksam umgesetzt sind. Die dafür von der Geschäftsleitung einzurichtende Risikomanagement-Organisation hat für eine neutrale und zeitnahe Risikoberichterstattung sowie für die dafür erforderliche wirksame Ausgestaltung des Risikomanagementsystems Sorge zu tragen.

36 Die Risikomanagementphasen finden in allen Teilen und auf allen Hierarchieebenen einer Organisation statt. Dies beinhaltet die Umsetzung der Risikostrategie, die Identifikation, Erfassung, Analyse, Bewertung, Steuerung und Überwachung sowie Berichterstattung bzw. Kommunikation der Risiken. Daher ist die Interaktion auf allen und über alle Ebenen hinweg durch eine geeignete Aufbauorganisation des Risikomanagements sicherzustellen. Dabei ist auf die erforderliche Qualifikation der im Risikomanagement Verantwortlichen zu achten. Die Interne Revision muss sich im Rahmen ihrer Prüfung von der Angemessenheit und Wirksamkeit dieser Aufbauorganisation überzeugen.

37 Ablauforganisation

Organisatorische Regelungen und Prozesse mit klarer Abgrenzung der Verantwortungsbereiche stellen sicher, dass ein angemessenes und wirksames Risikomanagementsystem etabliert ist.

38 Risikokultur

Basis für ein effektives Risikomanagementsystem ist eine Risikokultur, die einen offenen Umgang mit Risiken unterstützt. Damit wird nicht nur das Management bereits bekannter Risiken, sondern auch die schnelle Reaktion auf Änderungen im Risikoprofil unterstützt. Die Risikokultur umfasst als Teil der Unternehmenskultur die grundsätzliche Einstellung und das Verhalten beim Umgang mit Chancen und Risiken. Sie beeinflusst das Risikobewusstsein und bildet die Grundlage für ein wirksames Risikomanagementsystem im Unternehmen.

39 Die etablierten Abläufe im Risikomanagement sind von der Internen Revision auf ihre Angemessenheit und Wirksamkeit hin zu prüfen.

40 Dokumentation

Das Risikomanagementsystem ist z. B. in einem Risikomanagementhandbuch, welches die Eckpunkte des Systems wie Risikostrategie, Risikobewertung und Arbeitsanweisungen umfasst, zu dokumentieren. Dazu gehört auch die Beschreibung der operativen Umsetzung des Risikomanagementsystems in den verschiedenen Organisationseinheiten. Eine angemessene, systematische und für sachkundige Dritte nachvollziehbare Dokumentation der definierten Risikomanagementphasen ist Bestandteil der Prüfungen durch die Interne Revision.

6.2 Risikostrategie

41 Die Risikostrategie ist aus der Gesamtstrategie der Organisation abgeleitet. Sie umfasst die Risikobereitschaft der Geschäftsleitung unter Berücksichtigung des Risikode-

ckungspotenzials der Organisation, die Ziele der Risikosteuerung der wesentlichen Geschäftsaktivitäten sowie die Maßnahmen zur Erreichung dieser Ziele. Sie sollte so ausgestaltet sein, dass die operative Steuerung der Risiken daraus abgeleitet werden kann.

42 Für die Interne Revision ergeben sich folgende wesentliche Prüfungsaspekte:

- Konsistenz der Risikostrategie mit der Gesamtstrategie der Organisation,
- Konkretisierung in Bezug auf die Ableitung operativer Risikosteuerungsmaßnahmen,
- Darstellung aller wesentlichen und Berücksichtigung neuer Risiken; dazu gehört auch die Erfassung von Erkenntnissen über Risiken in allen Managementsystemen, beispielsweise aus dem Qualitätsmanagement und dem Informationssicherheitsmanagement, sowie der unsicheren Planannahmen im Rahmen von Planung und Budgetierung,
- Festlegung von Risikotoleranzen bzw. eines Limitsystems, welches in qualitativen oder quantitativen Vorgaben ausdrückt, in welchem Umfang die Geschäftsleitung bereit ist, bestimmte Risiken einzugehen,
- Darlegung des Risikotragfähigkeitskonzepts, welches darstellt, welche Ressourcen das Eingehen der tolerierten Risiken absichern,
- Einbezug der wesentlichen ausgelagerten Prozesse (Outsourcing) in die Risikobetrachtung,
- Regelmäßige und anlassbezogene Überprüfung und Anpassung der Risikostrategie,
- Adäquate Dokumentation und Kommunikation der Risikostrategie,
- Klare und operationale Definition des Begriffs der bestandsgefährdenden Entwicklung, um diese erkennen und ihre Wahrscheinlichkeit einschätzen zu können.

6.3 Risikoidentifikation und -erfassung

43 Die Risikoidentifikation und -erfassung umfasst eine methodische Ermittlung aller für die Aufgaben und Ziele der Organisation relevanten Risiken. Sie setzt an den von der Geschäftsleitung vorgegebenen Zielen und strategischen Entscheidungen an.

44 Eine Risikoinventur ist regelmäßig durchzuführen. Um neue oder im Umfang wesentlich veränderte Risiken früh zu erkennen, ist dabei insbesondere zu untersuchen, ob in den üblichen Arbeitsprozessen (z. B. der Budgetierung) implizit aufgedeckte Risiken auch im Risikomanagement berücksichtigt werden (Integriertes Risikomanagement). Je nach Geschäftsmodell der Organisation reicht dies von einer jährlichen Aufnahme und Bewertung der wesentlichen Risiken bis zu einer Echtzeit-Überwachung der Risiken. Die Identifikation

kann sowohl auf zentraler Ebene als auch dezentral durch zuständige Funktionen erfolgen. Die Möglichkeit zur angemessenen Strukturierung und Aggregation von Risiken ist dabei ebenso wichtig, wie die Berücksichtigung von Interdependenzen zwischen Risiken.

45 Zur Risikoidentifikation können zahlreiche Methoden und Instrumente eingesetzt werden, z. B. Unternehmens- und Umweltanalysen und Befragungen. Außer den Geschäftsprozessen sind auch die Unterstützungsprozesse wie Finanzen, Personal, Informationstechnologie sowie ausgelagerte Prozesse (Outsourcing) einzubeziehen. Besondere Beachtung finden müssen dabei die strategischen Risiken, die die wesentlichen Erfolgspotenziale bedrohen und die im Allgemeinen nur unter Einbeziehung der Geschäftsleitung analysiert werden können. Auch die systematische Erfassung von unsicheren Annahmen, die im Planungs- und Budgetierungsprozess, aber auch bei Entscheidungen im Kontext neuer Technologien gesetzt werden, ist eine wichtige Quelle der Risikoidentifikation. Darüber hinaus müssen die Methoden zur Identifikation seltener Risiken mit hohem Schadenspotenzial einbezogen werden. Bestandsgefährdende Entwicklungen hängen oft von solchen seltenen Extremrisiken (oder Kombinationseffekten von Risiken) ab, weshalb deren frühzeitige Erkennung wichtig ist.

46 Ergebnis der Risikoidentifikation und -erfassung sollte eine strukturierte und vorläufig priorisierte Darstellung aller identifizierten Risiken in einem Risikoinventar (Risikoregister, -katalog, -liste, -landkarte) sein.

47 Die Interne Revision prüft die Auswahl der eingesetzten Methoden und Instrumente zur Risikoidentifikation und bewertet deren Angemessenheit. Sie soll dabei auch darauf achten, ob das Risikoinventar in regelmäßigen Abständen auf Aktualität geprüft und entsprechend angepasst wird. Die Interne Revision untersucht, ob das Risikomanagementsystem alle wesentlichen Risiken erfasst, auch die Risiken infolge von Entscheidungen der Unternehmensführung.

48 Grundlage für die Prüfung der Vollständigkeit ist die Dokumentation der Risiken (Risikoinventar), die identifiziert wurden. Die Dokumentation der identifizierten Risiken sollte eine Aufzählung enthalten, welche Betriebsstellen, Geschäftsbereiche, Geschäftsfelder und Prozesse in die Risikoidentifikation einbezogen wurden und – ebenfalls explizit in einer Aufzählung benannt – welche nicht.

49 Die Prüfung der Vollständigkeit kann über einen Abgleich mit der Vorperiode, Interviews der Internen Revision mit den Verantwortlichen, Erkenntnisse aus vorherigen Revisionsaufträgen sowie die Einbeziehung externer Erfahrungswerte erfolgen. Darüber hinaus kann ein Abgleich der Erfassung mit historischen Schadensfällen oder mit wesentlichen Rückstellungen und einer ggf. vorhandenen Risikovorsorge vorgenommen werden. Abweichungsanalysen des Controllings zeigen die Ursachen eingetretener Planabweichungen, also die bereits eingetretenen Risiken, woraus Rückschlüsse auf die Vollständigkeit gezogen werden können.

6.4 Risikoanalyse und -bewertung

50 Die Analyse und Bewertung von Risiken und deren Aggregation erlauben eine Aussage zum Gesamtrisikoumfang (z. B. Eigenkapitalbedarf) und zu einer möglichen Bestandsgefährdung bzw. Auslastung des Risikodeckungspotenzials der Organisation. Bei der Risikoaggregation sind relevante Risikointerdependenzen zu berücksichtigen.

51 Die im Risikoinventar erfassten Risiken sind im Rahmen der Risikoanalyse hinsichtlich der Ursache-Wirkung-Zusammenhänge zu untersuchen sowie im Hinblick auf ihre Eintrittswahrscheinlichkeit und quantitativen Auswirkungen einzuschätzen. Dabei werden bei der Quantifizierung Netto-Risiken betrachtet, also die Risiken unter Berücksichtigung der vorhandenen Risikobewältigungsmaßnahmen. Das Aufzeigen des Brutto-Risikos ist im Hinblick auf die Schaffung von Transparenz sinnvoll, u. a. zur Identifikation von Schlüsselkontrollen. Die Risikoquantifizierung muss nachvollziehbar hergeleitet werden. Der Begriff der quantitativen Auswirkung umfasst mögliche positive und negative Abweichungen. Im Allgemeinen ist bei Eintreten eines Risikos die Auswirkung unsicher und durch eine Bandbreite und eine geeignete Wahrscheinlichkeitsverteilung zu beschreiben. Die Einschätzung der quantitativen Auswirkungen ist zu prüfen.

52 Die Quantifizierung von Risiken bezieht regelmäßig neben Benchmarks und historischen Schadensdaten auch subjektives Expertenwissen ein. Grundlage der Risikoquantifizierung sollten immer die besten verfügbaren Informationen sein bzw. die besten Informationen, die mit vertretbaren Kosten zu beschaffen sind. Da eine objektive Risikoquantifizierung häufig schwer möglich ist, ist die Datengrundlage zur Nachvollziehbarkeit der Quantifizierung von besonderer Bedeutung.

53 Die Risikotragfähigkeit kann oft auch über eine Abschätzung der maximalen Risikowirkung (z. B. in Euro), die eine Organisation überstehen kann, gemessen werden.

54 Damit wird die Risikotragfähigkeit über das wirtschaftliche Eigenkapital erfasst, das als Haftungsmasse zur Vermeidung einer Überschuldung zur Verfügung steht. Da Insolvenzen auch durch Zahlungsunfähigkeit ausgelöst werden, sind weitergehende Risikotragfähigkeitskonzepte sinnvoll.

55 Um Risiken zu priorisieren, Risikobewältigungsmaßnahmen zu beurteilen und Risiken in Handlungsalternativen (z. B. im Rahmen der Entscheidungsvorbereitung) einzubeziehen, ist es notwendig, die durch unterschiedliche quantitative Verfahren beschriebenen Risiken zu vergleichen. Die Interne Revision hat deshalb zu prüfen, ob dafür ein geeignetes Risikomaß verwendet wird, wie z. B. Value-at-Risk.

56 Aufgabe der Internen Revision im Rahmen der Prüfung der Risikoanalyse und -bewertung ist neben der Feststellung der vollständigen Durchführung der Analyse für alle

identifizierten Risiken vor allem die Beurteilung der Angemessenheit der angewandten Methoden. Darüber hinaus sind qualitative oder quantitative Analysen und Berechnungen in Stichproben nachzuvollziehen, um die korrekte Anwendung der Methoden festzustellen.

57 Bei Anwendung quantitativer Methoden ist besonders auf die Korrektheit der zugrundeliegenden Daten zu achten. Bei qualitativen Ansätzen sollte ein Schwerpunkt in der Prüfung der getroffenen Annahmen liegen.

58 Die Risikoquantifizierung ist die Beschreibung von Risiken mittels einer geeigneten Dichte- oder Verteilungsfunktion, mit historischen Daten (wie z. B. einer Liste der Schadensfälle) oder einer Häufigkeitsverteilung aus einer Monte-Carlo-Simulation. Ebenfalls zur Risikoquantifizierung gehört die Zuordnung von Risikomaßen. Möglich ist dabei die Beschreibung eines Risikos durch eine Wahrscheinlichkeitsverteilung, die die Wirkung in einer Periode angibt oder die Erfassung von zwei separaten Wahrscheinlichkeitsverteilungen, z. B. eine für die Häufigkeit und eine für die Schadenshöhe je Schadensfall. Bei der Risikoquantifizierung ist darauf zu achten, dass alle Risiken im Hinblick auf eine einheitliche Zielgröße (z. B. EBIT oder Ertrag) beschrieben werden. Werden in einem Zwischenschritt Risikowirkungen bezüglich mehreren Dimensionen (z. B. Zeit, Qualität und Kosten) erfasst, sollten diese schließlich auf eine Dimension verdichtet werden. Für privatwirtschaftliche Unternehmen ist dies im Allgemeinen die oberste ökonomische Zielgröße, z. B. Gewinn, Ertrag oder Unternehmenswert. Die Quantifizierung von Einzelrisiken ist notwendige Voraussetzung, um mittels Risikoaggregation den Gesamtrisikoumfang des betrachteten Prüfungsobjekts zu bestimmen. Der Gesamtrisikoumfang sollte durch geeignete Risikomaße ausgedrückt werden (z. B. Value at Risk, Eigenkapitalbedarf oder Variationskoeffizient der Erträge).

59 Bei der Prüfung kann der Revisor z. B. externe Statistiken oder Benchmarks heranziehen, um im Vergleich mit der zu beurteilenden Bewertung eines Risikoszenarios belastbare Resultate zu erzielen.

60 Die Methode der Risikoaggregation, die gewährleistet, dass auch die Kombinationseffekte von Einzelrisiken im Hinblick auf eine sich daraus ergebende bestandsgefährdende Entwicklung erkannt werden, ist zu prüfen.
Außerdem ist das Risikobewertungssystem im Rahmen der Prüfung zu beurteilen. Dazu gehören

- in Abhängigkeit von der Risikostrategie die Festlegung geeigneter Risikostufen,
- die angemessene Darstellung der Interdependenzen zwischen Risiken,
- die korrekte Durchführung der Aggregation von Risiken,
- ggf. die Ableitung eines Gesamtrisikos,
- die Aktualität von Risikobewertungen.

Basis dafür ist eine nachvollziehbare Dokumentation des Risikobewertungssystems sowie der Analysen und Ergebnisse.

6.5 Risikosteuerung und -überwachung

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). Durch Maßnahmen der Risikoüberwachung lassen sich die Veränderungen der Risiken im Zeitablauf messen und die Risikosteuerung anpassen. Die Interne Revision dient als unabhängige Prüfungsinstanz für das Risikomanagementsystem.

62 Die Risikosteuerung beschäftigt sich mit den Maßnahmen, die durchzuführen sind, um die identifizierten und analysierten Risiken im Sinne der Risikostrategie zu steuern. Die Steuerungsmaßnahmen orientieren sich an der Risikostrategie der Organisation und können die Risikovermeidung (Einstellung bzw. Unterlassung von Aktivitäten), Risikoübertragung (Lieferanten, Kunden, Kapitalmarkt, Versicherungen), Risikoreduktion (markt- oder prozessorientierte Maßnahmen) oder Risikoakzeptanz zum Ziel haben. Sie setzen bei den Risikoauswirkungen, bei der Eintrittswahrscheinlichkeit oder bei beiden Größen an und sind darauf ausgerichtet, dass die Organisationsziele erreicht werden und der Fortbestand der Organisation nicht gefährdet wird.

63 Es bietet sich an, für relevante Risiken Indikatoren und zugehörige Grenzwerte zu definieren, mit denen sich Veränderungen eines Risikos im Zeitablauf messen und beurteilen lassen. Sie werden kontinuierlich überwacht, um frühzeitig erkennen zu können, ob ein kritischer Risikoumfang überschritten wird.

64 Die Interne Revision hat bei der Prüfung die Angemessenheit und Wirksamkeit der Maßnahmen und Kontrollen zur Risikosteuerung zu beurteilen. Aufgrund der hohen Bedeutung der Risikosteuerung für das Risikomanagementsystem insgesamt ist durch angemessene Prüfungshandlungen und Stichproben eine ausreichende Prüfungssicherheit zu gewährleisten. Dazu gehört die Beurteilung der

- Beschreibung der definierten Indikatoren, Steuerungsmaßnahmen, Kontrollen und Überwachungsmaßnahmen (Ist diese systematisch und für sachkundige Dritte nachvollziehbar?),
- Angemessenheit und Wirksamkeit der Nutzung von Risikoindikatoren zur frühzeitigen Risikoidentifikation sowie von definierten Grenzwerten, u. a. vor dem Hintergrund der freien Risikotragfähigkeit,

- Eignung der implementierten Risikosteuerungsmaßnahmen (Wirken diese tatsächlich wie gewünscht auf das Risiko ein? Wird die Risikostrategie umgesetzt?),
- Eignung der implementierten Kontrollen (Können diese sicherstellen, dass die vom Management festgelegten Risikosteuerungsmaßnahmen korrekt und zeitgerecht durchgeführt werden?),
- Wirtschaftlichkeit gewählter Maßnahmen und Kontrollen zur Steuerung der identifizierten Risiken,
- Angemessenheit und Wirksamkeit der prozessintegrierten und prozessunabhängigen Überwachungsaktivitäten in der First und Second Line of Defense. (Werden die Risikoindikatoren beobachtet und weiterentwickelt? Werden neue Einflüsse auf die Risikostrategie berücksichtigt? Wird das Vorhandensein und Funktionieren der einzelnen Risikomanagementphasen laufend oder periodisch beurteilt? Herrscht Transparenz über die identifizierten Schwachstellen und den Verbesserungsprozess?)

6.6 Risikoberichterstattung und -kommunikation

65 Das wesentliche Ziel der Risikoberichterstattung und -kommunikation ist, den Entscheidungsträgern und Aufsichtsorganen zeitnah die Risikolage der Organisation widerzuspiegeln. Dabei muss über den Gesamtrisikoumfang und die Wahrscheinlichkeit einer bestandsgefährdenden Entwicklung informiert werden. Dabei sind sowohl regelmäßige Berichte als auch Ad-hoc-Risikomeldungen im konkreten Bedarfsfall zu berücksichtigen. Es ist insbesondere sicherzustellen, dass bei der Vorbereitung wesentlicher Entscheidungen die Risikoinformationen für diese Entscheidung zur Verfügung stehen.

66 Aufbau des Risikomanagementsystems, Ergebnis der Risikoinventur und die Beschreibung des implementierten Überwachungssystems, das die Einhaltung der eingeleiteten Maßnahmen zur laufenden Erfassung, Steuerung und Kommunikation von Risiken gewährleistet, werden regelmäßig an die Geschäftsleitung und das Aufsichtsorgan berichtet. Bestandteil dieser Berichterstattung sollten auch Aussagen zu identifizierten Schwächen in Organisation und Methoden des Risikomanagementsystems sowie zu dessen Wirksamkeit sein.

67 Für die Ad-hoc-Risikomeldungen sollten Schwellenwerte sowie ggf. weitere Bedingungen definiert werden. Dabei kann die Ad-hoc-Berichterstattung neben der Risikolage auch Informationen zu identifizierten Schwachstellen und zur Funktionsfähigkeit des Risikomanagementsystems enthalten.

68 Für Aufsichtsräte ist die Risikoberichterstattung ein wichtiges Instrument im Rahmen der Erfüllung ihrer gesetzlichen Überwachungspflicht, die auch die Wirksamkeit des Risikomanagementsystems zum Inhalt hat.

69 Die Interne Revision muss die Berichterstattung in ihre Prüfungshandlungen einbeziehen. Gegenstand der Prüfung der Internen Revision ist einerseits die Angemessenheit der Vorgaben für die interne Risikoberichterstattung und -kommunikation und andererseits die wirksame Umsetzung dieser Vorgaben in der Praxis. Ebenfalls Gegenstand der Prüfung des Berichtswesens sind Entscheidungsvorlagen (z. B. bei Investitionen), da auch hier geprüft werden kann, inwieweit aussagefähige Risikoinformationen bei der Entscheidungsvorbereitung vorlagen.

70 Es ergeben sich folgende wesentliche Prüfungsaspekte:

- Festgelegte Rahmenbedingungen für die Berichterstattung: Hierzu zählen Festlegungen was zu berichten ist (z. B. Risiken, Risikobewertungen, Steuerungsmaßnahmen, Indikatoren, Entwicklungstendenz), welche Risikokategorien genannt werden, welche Wesentlichkeitsgrenzen beachtet werden, welcher Berichtszyklus und welches Berichtsmedium angewendet wird sowie ob eine Brutto- oder Nettorisikoberichterstattung erfolgt.
- Für Regel- und Ad-hoc-Berichterstattung müssen der Kommunikationsprozess, die jeweiligen Verantwortlichen für die Berichterstattung sowie die Berichtsempfänger bestimmt sein. Auch für gesetzliche Meldeverpflichtungen (z. B. börsenrechtliche Ad-hoc-Meldungen) muss ein geeigneter Prozess eingerichtet sein.
- Anhand von Stichproben ist die Einhaltung der Vorgaben bei der Kommunikation zu prüfen.
- Gegenstand der Prüfung ist auch, ob die Berichterstattung insgesamt verständlich, vollständig, zeitnah und entscheidungsrelevant bzw. adressatengerecht ist. Die Darstellung der Aggregation von Risiken und die notwendige Transparenz und Aussagekraft sind zu beurteilen.
- Zentraler Aspekt ist dabei die Prüfung der Bereitstellung der Ergebnisse aus der Risikoaggregation, um bestandsgefährdende Entwicklungen aus der Kombination mehrerer Einzelrisiken zu erkennen.
- Die Berücksichtigung von Risikoinformationen bei wesentlichen unternehmerischen Entscheidungen (z. B. in Entscheidungsvorlagen bei der Geschäftsleitung) muss nachvollziehbar sein.

Autoren

Erarbeitet im gemeinsamen DIIR- und RMA-Arbeitskreis „Interne Revision und Risikomanagement“

DIIR – Deutsches Institut für Interne Revision e.V.
Theodor-Heuss-Allee 108
60486 Frankfurt am Main

Veröffentlicht im November 2018 auf www.diir.de

Version 2.0