DIIR Revisionsstandard Nr. 2

Prüfung des Risikomanagementsystems durch die Interne Revision

Veröffentlicht im August 2014 und geändert im September 2015
(Version 1.1), Frankfurt am Main

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. Wie im Three Lines of Defense-Modell dargestellt, hat die Interne Revision als Third Line auch die Prozesse der Funktionen in der Second Line (z. B. Compliance, Risikomanagement, Controlling) 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.

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 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

6 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.

7 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

8 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]).

9 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.

10 Für die Finanzbranche werden durch die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) verschiedene Mindestanforderungen an das Risikomanagement (MaRisk) festgelegt. Hierin werden 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 niedergelegt. Außerdem wird dort ein Rahmen für die Ausgestaltung der Internen Revision vorgegeben.

11 Für die öffentlichen Bereiche ergibt sich die Verpflichtung zu einem Risikomanagement aus § 53 des Haushaltsgrundsätzegesetzes sowie in der Bundeshaushaltsordnung, den Landeshaushaltsordnungen und den Gemeindeordnungen der jeweiligen Länder.

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

4 Begriffsdefinitionen

13 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.

14 **Risiko**

Der Begriff Risiko beschreibt die Möglichkeit des Eintretens von Ereignissen oder von Entwicklungen, die sich auf das Erreichen von Zielen negativ auswirken. Ein Risiko entsteht infolge der bestehenden Unsicherheiten oder der unvollständigen Informationen in Bezug auf die zukünftige Entwicklung von Zielgrößen. Exemplarische Risikokategorien sind strategische Risiken, operative Risiken, Berichterstattungs- sowie Compliancerisiken.

15 **Risikomanagement**

Risikomanagement bezeichnet alle Tätigkeiten, die darauf ausgerichtet sind, Risiken frühzeitig und systematisch zu erfassen, zu steuern und zu überwachen, um das Erreichen der Organisationsziele zu gewährleisten. 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.

16 **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, Verantwortlichkeiten und Kompetenzen, in denen die Geschäftsprozesse inklusive der Risikomanagementtätigkeiten ablaufen. Dies kann strategische Planung, Entscheidungsprozesse und andere Prozesse, die sich mit Risiken beschäftigen, beinhalten. Das Risikomanagementsystem ist regelmäßig weiterzuentwickeln und zu überwachen.

17 **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.

5 Auftrag der Internen Revision zur Prüfung des Risikomanagementsystems

18 Zu einer erfolgreichen und wertorientierten Führung einer Organisation im Sinne einer guten Corporate Governance gehört ein auf die Risikolage fokussierendes Überwachungssystem.

19 Die sich daraus abzuleitende 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."

20 Die Internationalen Standards für die berufliche Praxis der Internen Revision (International Professional Practices Framework) 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."

21 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

22 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.

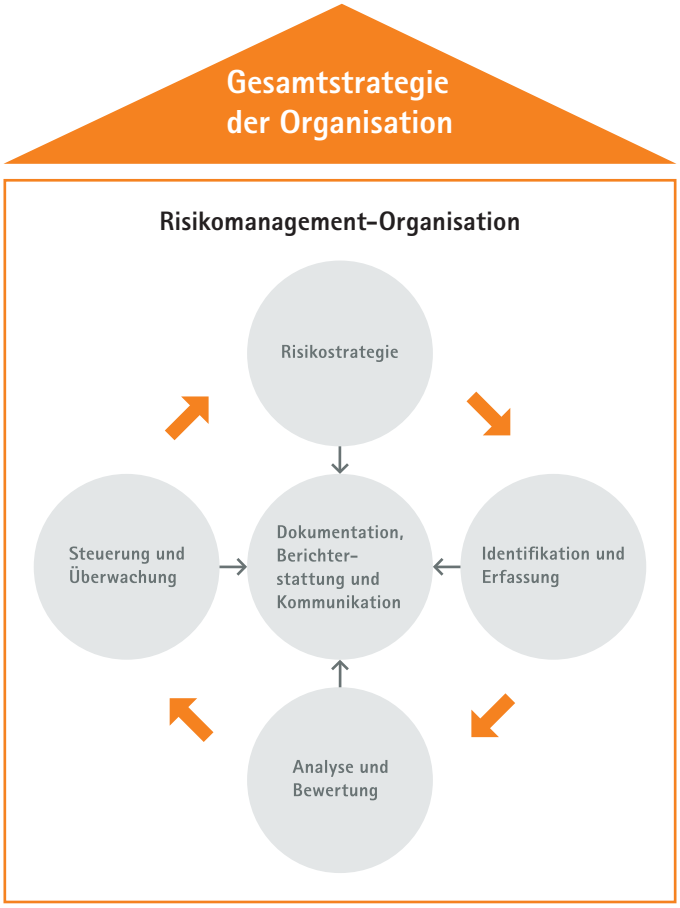

Abbildung 1: Phasenmodell des Risikomanagements

23 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 zwei Komponenten in der Prüfung wichtig: die Aufbauprüfung und die Funktionsprüfung.

24 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, Anpassungsfähigkeit (Dynamik) und Integration in bestehende Überwachungs- und Führungssysteme.

25 Durch die Funktionsprüfung 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. Die Prüfung kann auf eine Auswahl von Risiken beschränkt werden, da eine Vollprüfung in vielen Fällen nicht erforderlich (risikoadäquater Prüfungsschwerpunkt) und daher mit Blick auf das Aufwand-Nutzen-Verhältnis nicht vertretbar ist.

6.1 Risikomanagement-Organisation

26 **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.

27 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.

28 **Ablauforganisation**

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

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

30 **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

31 Die Risikostrategie ist aus der Gesamtstrategie der Organisation abgeleitet. Sie umfasst den Risikoappetit (die Risikobereitschaft) der Geschäftsleitung unter Berücksichtigung der Risikotragfähigkeit 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.

32 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,
- 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 bzw. Haftungsmassen 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.

6.3 Risikoidentifikation und -erfassung

33 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.

34 Eine Risikoinventur ist regelmäßig durchzuführen. 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 Aggregation von Risiken ist dabei ebenso wichtig, wie die Möglichkeit zur Berücksichtigung von Interdependenzen zwischen Risiken.

35 Zur Risikoidentifikation können zahlreiche Methoden und Instrumente eingesetzt werden, z. B. Unternehmens- und Umweltanalysen, Befragungen. Außer den Geschäftsprozessen sind auch die Unterstützungsprozesse wie Finanzen, Personal, Informationstechnologie sowie ausgelagerte Prozesse (Outsourcing) einzubeziehen.

36 Ergebnis der Risikoidentifikation und -erfassung ist eine strukturierte Darstellung aller identifizierten Risiken in einem Risikoinventar (Risikoregister, -katalog, -liste, -landkarte).

37 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.

38 Die Interne Revision untersucht, ob das Risikomanagementsystem alle wesentlichen Risiken erfasst, wobei auch die in die Zukunft reichenden strategischen Entscheidungen mit den dazugehörenden Risiken zu betrachten sind. 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.

39 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.

6.4 Risikoanalyse und -bewertung

40 Ziel der Risikoanalyse und -bewertung ist die Priorisierung von Steuerungsmaßnahmen durch eine geeignete Risikomessung. Die Bewertung von Risiken und deren Aggregation erlauben eine Gesamtaussage zur Risikolage der Organisation und zu einer möglichen Bestandsgefährdung bzw. Auslastung der Risikotoleranz. Hierbei sind auch relevante Risikointerdependenzen zu berücksichtigen.

41 Die im Risikoinventar erfassten Risiken sind im Rahmen der Risikoanalyse hinsichtlich der Ursache-Wirkung-Zusammenhänge zu untersuchen sowie im Hinblick auf ihr Schadenspotenzial und ihre Eintrittswahrscheinlichkeit einzuschätzen. Das Schadenspotenzial kann hinsichtlich monetärer oder nicht-monetärer Auswirkungen beurteilt werden. Die Einschätzung kann qualitativ (z. B. Expertenschätzung), semi-quantitativ (z. B. mit Hilfe von Scoring-Modellen) oder durch quantitative Messung (z. B. Monte-Carlo-Simulation) vorgenommen werden.

42 Die Risikobewertung erfolgt z. B. in Form eines Risiko-Rankings oder durch Einordnung in eine Risikomatrix, in der Schadenspotenzial und Eintrittswahrscheinlichkeiten in angemessen vielen Risikostufen abgebildet werden können. Bei der Risikobewertung wird das Brutto- vom Nettorisiko unterschieden. Bei der Bewertung des Nettorisikos werden – im Gegensatz zum Bruttorisiko – die Auswirkungen von risikomindernden Steuerungsmaßnahmen berücksichtigt, die Schadenspotenzial und/oder Eintrittswahrscheinlichkeit beeinflussen.

43 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.

44 Bei Anwendung quantitativer Methoden ist besonders auf die Korrektheit der zugrunde liegenden Daten zu achten. Bei qualitativen Ansätzen sollte ein Schwerpunkt der Prüfung in der Verifizierung der Annahmen liegen.

45 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.

46 Das Risikobewertungssystem ist 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

47 Die Risikosteuerung beschäftigt sich mit den Maßnahmen, die durchzuführen sind, um die identifizierten und analysierten Risiken im Sinne der Risikostrategie zu steuern.

48 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.

49 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 entweder beim Schadenspotenzial, bei der Eintrittswahrscheinlichkeit oder bei beiden Größen an und sind letztlich darauf ausgerichtet, dass die definierten Ziele erreicht werden und der Fortbestand der Organisation nicht gefährdet wird.

50 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 kritische Toleranzgrenzen überschritten werden.

51 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 gehören 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 des Risikoappetits (der Risikobereitschaft) der Organisation,
- Eignung der implementierten Risikosteuerungsmaßnahmen (Wirken diese tatsächlich wie gewünscht auf das Risiko ein? Wird die Risikostrategie umgesetzt? Bleibt das Restrisiko innerhalb vereinbarter Grenzwerte?),

- 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

52 Das wesentliche Ziel der Risikoberichterstattung und -kommunikation ist, den Entscheidungsträgern und Aufsichtsorganen zeitnah die Risikolage der Organisation widerzuspiegeln. Dabei sind sowohl regelmäßige Berichte als auch Ad-hoc-Risikomeldungen im konkreten Bedarfsfall zu berücksichtigen.

53 Aufbau des Risikomanagementsystems, Ergebnis der Risikoinventur und die Beschreibung eines geeigneten 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 im Risikomanagementsystem sowie zu dessen Wirksamkeit sein.

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

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

56 Die Interne Revision muss die Berichterstattung in ihren Prüfungsumfang 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.

57 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.

DIIR

Deutsches Institut für
Interne Revision e.V.

Ohmstraße 59
60486 Frankfurt am Main
Telefon (069) 71 37 69 - 0
Fax (069) 71 37 69 - 69
www.diir.de
info@diir.de