



DIIR

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

Version 2.2, August 2026

Inhalt

1	Präambel.....	3
2	Adressaten, Geltungsbereich und Verbindlichkeit des Standards	5
3	Rechtliche Grundlagen des Risikomanagementsystems.....	6
4	Begriffsdefinitionen	7
5	Auftrag der Internen Revision zur Prüfung des Risikomanagementsystems	10
6	Prüfung des Risikomanagementsystems und seiner Phasen.....	12
6.1	Phasenmodell des Risikomanagements.....	12
6.2	Risikomanagement-Organisation und Risikokultur	13
6.3	Risikostrategie	15
6.4	Risikoidentifikation und -erfassung	16
6.5	Risikoanalyse und -bewertung.....	17
6.6	Risikosteuerung und -überwachung	20
6.7	Risikoberichterstattung und -kommunikation	21
7	Prüfung unternehmerischer Entscheidungen unter Risiko.....	23

1 Präambel

1 Das unternehmensweite 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 Model hat die Interne Revision als Third Line neben der First Line (operatives Management) auch die Prozesse und Struktur 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 Prüfungshandlungen umzusetzen. Dabei wird die Einbeziehung von Risikomanagementstandards, z. B. COSO ERM Integrated Framework oder ISO 31000, empfohlen.

5 Die Prüfung muss auch die gesetzlichen Anforderungen aus § 91 Abs. 2-3, § 107 Abs. 3-4 AktG und § 1 StaRUG 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 solche Unternehmen, die nicht unmittelbar vom Gesetzeswortlaut erfasst werden.

6 Mit dem am 01.01.2021 in Kraft getretenen Gesetz über den Stabilisierungs- und Restrukturierungsrahmen für Unternehmen (StaRUG) wird klargestellt, dass analog § 91 Abs. 2 AktG die Geschäftsleitungen aller Gesellschaften ohne natürliche Personen als

Vollhafter, speziell damit auch GmbH und GmbH & Co. KG, verpflichtet sind, mögliche bestandsgefährdende Entwicklungen zu erkennen. Erstmals wird von der Geschäftsleitung gefordert, bei einer kritischen Bestandsgefährdung nun geeignete Gegenmaßnahmen der Krisen- und Risikobewältigung, bis hin zu einem Restrukturierungsplan zu ergreifen. Die Entscheidung über solche Gegenmaßnahmen ist grundsätzlich als eine unternehmerische Entscheidung im Sinne von § 93 AktG aufzufassen.

7 Bei solchen, wie auch bei anderen unternehmerischen Entscheidungen (z. B. bedeutenden Investitionen), fordert der Gesetzgeber, dass das Leitungsorgan auf Basis angemessener Informationen handelt, damit im Falle eines Schadeneintritts die Business Judgement Rule greifen kann und das Leitungsorgan nicht mangels Pflichtverletzung persönlich haftet.¹ Insbesondere ist bei der Entscheidungsvorbereitung aufzuzeigen, welche Chancen und Gefahren (Risiken) mit der beabsichtigten Entscheidung verbunden sind und wie sich der Risikoumfang durch die Entscheidung verändern würde. Die infolge § 93 AktG notwendige entscheidungsorientierte Ausrichtung des Risikomanagements ist folglich auch Prüfungsgegenstand. Aufgrund der hohen Bedeutung von unternehmerischen Entscheidungen unter Risiko wurde diesem Revisionsstandard ein ergänzendes Kapitel 7 gewidmet.

8 Außerdem wurden die Implikationen des am 01.07.2021 in Kraft getretenen Gesetzes zur Stärkung der Finanzmarktintegrität (FISG) berücksichtigt. Wesentlich ist hier insbesondere die Erweiterung von § 91 AktG um Abs. 3: „Der Vorstand einer börsennotierten Gesellschaft hat darüber hinaus ein im Hinblick auf den Umfang der Geschäftstätigkeit und die Risikolage des Unternehmens angemessenes und wirksames internes Kontrollsystem und Risikomanagementsystem einzurichten.“ Die Anforderung an das Risikomanagement und die internen Kontrollsysteme von börsennotierten Aktiengesellschaften werden hier ausdrücklich erwähnt und im Aufgabenumfeld konkretisiert. Damit ergeben sich für die börsennotierten Aktiengesellschaften Anforderungen, die über die allgemeinen Anforderungen aus § 1 StaRUG hinausgehen. Für die Interne Revision börsennotierter Aktiengesellschaften bedeutet dies, dass die Angemessenheit und Wirksamkeit eines umfassenden Risikomanagementsystems und eines internen Kontrollsystems zu prüfen sind. Neben der Risikofrüherkennung umfasst dieses insbesondere auch die Risikobewältigung und die Einbeziehung von Risikoanalysen bei unternehmerischen Entscheidungen.

9 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.

¹ Eine Pflichtverletzung liegt nicht vor, wenn das Vorstandsmitglied bei einer unternehmerischen Entscheidung vernünftigerweise annehmen durfte, auf der Grundlage angemessener Information zum Wohle der Gesellschaft zu handeln. (§ 93 Abs. 1 AktG, Business Judgement Rule)

2 Adressaten, Geltungsbereich und Verbindlichkeit des Standards

10 Der vorliegende Standard richtet sich vorrangig an Leiter und Mitarbeiter von Internen Revisionen. 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.

11 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

12 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 Vorschriften (bspw. Handelsgesetz und Aktiengesetz), aber auch aus branchenspezifischen Regelungen (bspw. die Mindestanforderungen an das Risikomanagement (MaRisk) in der Finanzbranche).

13 Während im Handelsrecht (§§ 289 und 315 HGB) die Berichtspflichten über das Risikomanagementsystem im Lagebericht beschrieben werden, fordert insbesondere das Aktiengesetz in § 91 (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. Durch das FISG wurde das Aktiengesetz um konkrete Anforderungen zu Umfang und Wirksamkeit des internen Kontrollsystems und Risikomanagementsystems erweitert (siehe auch Tz. 8).

14 Die Regelungen des Aktiengesetzes haben für Organisationen anderer Rechtsformen je nach Größe, Komplexität und Struktur eine Ausstrahlungswirkung. Nach § 1 StaRUG sind seit 01.01.2021 explizit die Geschäftsleiter aller Organisationen ohne natürliche Person als Vollhafter, speziell also der GmbHs und GmbH & Co. KGs, verpflichtet, Entwicklungen zu überwachen, die zu einer Bestandsgefährdung führen können.

15 Für die Finanzbranche wurden durch deutsche und europäische Aufsichtsbehörden Grundsätze für die Ausgestaltung des Risikomanagements, spezifische Anforderungen an die Organisation und die Prozesse für das Management und das Controlling von Risiken sowie Regelungen für die Ausgestaltung der Internen Revision vorgegeben.

16 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.

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

4 Begriffsdefinitionen

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

19 Risiko

Der Begriff Risiko beschreibt die Möglichkeit des Eintretens von Ereignissen oder von Entwicklungen, die sich auf die Erreichung von Zielen auswirken, was die Möglichkeit von positiven Abweichungen (Chancen) und negativen Abweichungen (Gefahren, Risiken im engeren Sinn) einschließt. Analyse und Quantifizierung von Risiken setzen 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 des Umfeldes der Zielgrößen. Die meisten regulatorischen Anforderungen beziehen sich primär auf Gefahren oder Verlustrisiken, während der symmetrische Risikobegriff eher dem betriebswirtschaftlichen Entscheidungskalkül dient. Exemplarische Risikokategorien sind strategische Risiken, Marktrisiken, operative Risiken, Berichterstattungs- sowie Compliancerisiken. Wesentliche Risiken ergeben sich für Unternehmen aus strategischen Zielsetzungen, beispielsweise im Bereich Cybersicherheit, Einsatz von künstlicher Intelligenz, Digitalisierung oder Nachhaltigkeit.

20 Risikomanagement

Risikomanagement bezeichnet alle Tätigkeiten, die darauf ausgerichtet sind, Risiken frühzeitig und systematisch zu erfassen, zu steuern und zu überwachen. Neben bereits vorhandenen Risiken sind durch das Risikomanagement insbesondere auch geplante Maßnahmen und Entscheidungen und deren mögliche Risiken zu betrachten. Die alleinige Überwachung schon identifizierter Risiken ist unzureichend. Somit gehören zum Risikomanagement 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.

21 Ein unternehmensweites Risikomanagement entsprechend den Anforderungen für börsennotierte Aktiengesellschaften nach § 91 Abs. 2-3 AktG umfasst neben dem Risikofrüherkennungssystem und der Risikosteuerung bzw. Risikobewältigung insbesondere auch die Einbeziehung von Risikoanalysen bei unternehmerischen Entscheidungen (§ 93 AktG).

22 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. In seinen wesentlichen Teilen muss es schriftlich, zum Beispiel in einer Richtlinie, niedergelegt sein.

23 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 ermöglicht wird und potenzielle, die Organisation wesentlich beeinflussende Ereignisse erkannt werden können und darauf angemessen reagiert werden kann.

24 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 gemäß § 91 Abs. 2 AktG und § 1 StaRUG zu erkennen.

25 Die Risikoaggregation erlaubt die Berechnung von Kennzahlen für den Gesamtrisikoumfang (Value-at-Risk oder Eigenkapitalbedarf) und daraus ableitbare Größen (wie Insolvenzwahrscheinlichkeit oder risikogerechte Kapitalkosten). Einzelrisiken sind nicht einfach addierbar. Insbesondere durch die Monte-Carlo-Simulation, aber auch durch gleichwertige stochastische Methoden, ist es möglich, unterschiedliche Risikotypen (beschrieben durch unterschiedliche Wahrscheinlichkeitsverteilungen) zu aggregieren. Mit Blick auf ihre Unternehmensplanung können sich Organisationen so ein besseres Gesamtbild der Risikolage verschaffen.

26 Gesamtrisikoumfang, Risikodeckungspotenzial, Risikotragfähigkeit, Risikotoleranz

Es empfiehlt sich, Kennzahlen zu definieren, die den aggregierten Gesamtrisikoumfang in Relation zum Risikodeckungspotenzial des Unternehmens setzen. Das Risikodeckungspotenzial lässt sich auf zweierlei Weise definieren: a) das vorhandene Eigenkapital zur Abdeckung möglicher Verluste und b) die Liquiditätsreserven (inkl. freier und möglicher zusätzlicher Kreditlinien) zur Abdeckung risikobedingter Liquiditätsabflüsse. Die

Liquiditätsreserven sind zumeist die für den Unternehmensfortbestand entscheidende Größe.

27 Die Risikotragfähigkeit ergibt sich aus dem Risikodeckungspotenzial und dem aggregierten Gesamtrisikoumfang. Kennzahlen für die Risikotragfähigkeit beurteilen den Grad der Bestandsgefährdung bzw. die Wahrscheinlichkeit für eine bestandsgefährdende Entwicklung (vergleiche Tz. 29).

28 Während sich die Risikotragfähigkeit damit auf eine bestandsgefährdende Entwicklung bezieht, stellt die Risikotoleranz auf ein vorsichtigeres, von der Geschäftsleitung festgelegtes Sicherheitsziel ab. Für die Beurteilung der Risikotoleranz wird die Angabe vergleichbarer Kennzahlen empfohlen, wie sie für die Beurteilung der Risikotragfähigkeit verwendet werden (z. B. die Wahrscheinlichkeit, das festgelegte Sicherheitsziel zu verletzen).

29 Bestandsgefährdende Entwicklung

Von einer bestandsgefährdenden Entwicklung spricht man, wenn eine Situation der Überschuldung oder Zahlungsunfähigkeit droht. Zahlungsunfähigkeit droht, wenn nicht ausreichend schnell liquidierbare Vermögensmassen vorhanden sind und Kreditvereinbarungen (Covenants) verletzt werden, die eine Kündigung von Krediten nach sich ziehen, und/oder Mindestanforderungen der Fremdkapitalgeber an das Rating nicht mehr erfüllt sind. Grundsätzlich kann man von einer bestandsgefährdenden Entwicklung im Sinne § 91 Abs. 2 AktG bzw. § 1 StaRUG ausgehen, wenn die Geschäftsleitung nicht mehr allein in der Lage ist, eine schwere Krise abzuwenden (also z. B. auf eine Kapitalerhöhung durch die Gesellschafter oder ein vertraglich nicht abgesichertes Entgegenkommen von Gläubigern angewiesen ist). Wird dieser kritische Grad der Bestandsgefährdung überschritten, sind geeignete Gegenmaßnahmen durch die Geschäftsleitung (Vorstand oder Geschäftsführer) zu initiieren und das Überwachungsorgan (i. d. R. der Aufsichtsrat) über die Situation und die geplanten Maßnahmen zu informieren.

30 Früherkennung der Bestandsgefährdung

Die Geschäftsleiter haftungsbegrenzter Unternehmen sind zur Etablierung geeigneter Verfahren zur Früherkennung bestandsgefährdender Risiken verpflichtet. Dabei müssen zumindest mögliche bestandsgefährdende Entwicklungen frühzeitig erkannt werden. Gerade bei einer Früherkennung kann es nicht nur darum gehen, finanzielle Warnsignale (siehe Tz. 29) wahrzunehmen. Denn beispielsweise ein Lieferengpass oder mangelndes Kundeninteresse sind frühe Indikatoren, die sich jedoch noch nicht in der Liquidität oder der Buchhaltung niedergeschlagen haben. Ein solches Früherkennungssystem fokussiert sich auf schwache Signale. Krisenfrüherkennung und Krisenprävention beziehen sich hingegen auf bestandsgefährdende Entwicklungen als Resultat realisierter Risiken. In diesem DIIR-Revisionsstandard werden sowohl die Früherkennung der Bestandsgefährdung als auch die Krisenprävention als Gegenstände einer Prüfung durch die Interne Revision betrachtet.

5 Auftrag der Internen Revision zur Prüfung des Risikomanagementsystems

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

32 Die sich daraus ergebende Aufgabe der Internen Revision, das Risikomanagement umfassend zu prüfen, spiegelt sich in deren Definition im Glossar der Global Internal Audit Standards des Institute of Internal Auditors (IIA) wider:

„Interne Revision: Eine unabhängige und objektive Prüfungs- und Beratungstätigkeit, welche darauf ausgerichtet ist, Mehrwerte zu schaffen und die Geschäftsprozesse zu verbessern. Sie hilft einer Organisation, ihre Ziele zu erreichen, indem sie einen systematischen und zielgerichteten Ansatz zur Bewertung und Verbesserung der Wirksamkeit der Governance-, Risikomanagement- und Kontrollprozesse anwendet.“

33 Die Global Internal Audit Standards nennen im Standard 9.4 die Aufgabe der Internen Revision bzgl. der Prüfung des Risikomanagements:

„Der Revisionsplan muss [...] Revisionsleistungen spezifizieren, die die Bewertung und Verbesserung der Governance-, Risikomanagement- und Kontrollprozesse der Organisation unterstützen. [...]“

34 Ergänzend zu den Standards hat das IIA im Rahmen der Internationalen Grundlagen für die berufliche Praxis den Global Practice Guide „Assessing the Risk Management Process“ veröffentlicht und zur Anwendung empfohlen.

35 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. Bislang untersuchen die Abschlussprüfer gemäß dem IDW Prüfungsstandard 340 n.F. (01.2022) lediglich die gesetzlichen Anforderungen an das Vorhandensein eines Risikofrüherkennungssystems nach § 91 Abs. 2 AktG. Eine erweiterte Prüfung von Risikomanagementsystemen durch den Wirtschaftsprüfer gemäß IDW PS 981 ist hingegen freiwillig und nicht Bestandteil der Abschlussprüfung. Aus § 93 AktG und § 1 StARUG sowie dem FISG ergeben sich weitere Anforderungen an das Risikomanagement. Diese müssen ebenfalls im Fokus der Internen Revision sein. Sie werden deshalb in diesem DIIR-Revisionsstandard erfasst und in Kapitel 6 näher thematisiert.

36 Bei börsennotierten Aktiengesellschaften ist zudem zu prüfen, ob ein angemessenes und wirksames internes Kontrollsystem und Risikomanagementsystem existieren (§ 91 Abs. 3 AktG). Daher sind hier auch die Verfahren für Risikosteuerung und Risikobewältigung Gegenstand der Prüfung. Betrachtet werden sollten dabei die Angemessenheit und Wirksamkeit der Verfahren und die Kosten dieser Verfahren im Vergleich zur erwarteten Risikoreduzierung. Die Prüfung des Risikomanagements nach diesem DIIR-Revisionsstandard geht über eine Prüfung durch den Abschlussprüfer nach IDW PS 340 n.F. (01.2022) hinaus.

6 Prüfung des Risikomanagementsystems und seiner Phasen

6.1 Phasenmodell des Risikomanagements

37 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

38 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.

39 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 sowie der Datenintegrität, Dokumentation, Anpassungsfähigkeit (Dynamik) und Integration in bestehende Überwachungs- und Führungssysteme.

40 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 Kombinationseffekten von Einzelrisiken zu erkennen. Ebenso zu prüfen sind die Methoden zur Berücksichtigung von Risikoinformationen bei der Entscheidungsvorbereitung.

41 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.

42 Der ergänzende Prüfungsleitfaden zum DIIR-Revisionsstandard Nr. 2 kann als Hilfestellung für die Interne Revision in der Praxis genutzt werden.

6.2 Risikomanagement-Organisation und Risikokultur

43 Aufbauorganisation

Die Verantwortung für das Risikomanagementsystem liegt bei der Geschäftsleitung. 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.

44 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.

45 Ablauforganisation

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

46 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 Gefahren. Sie beeinflusst das Risikobewusstsein und bildet die Grundlage für ein wirksames Risikomanagementsystem im Unternehmen. Prüfungshandlungen könnten die Auswertung von Hinweisgebersystemen, eine Tone-at-the-top-Analyse oder die Befragung des Personals zum Risikobewusstsein umfassen.

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

48 Dokumentation

Das Risikomanagementsystem ist z. B. in einem Risikomanagementhandbuch oder einer Richtlinie, die die Eckpunkte des Systems wie Risikostrategie, Risikobewertung und Arbeitsanweisungen umfassen, 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.

6.3 Risikostrategie

49 Die Risikostrategie ist aus der Gesamtstrategie der Organisation abgeleitet. Sie umfasst die Risikobereitschaft der Geschäftsleitung unter Berücksichtigung des Risikodeckungspotenzials 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.

50 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, und Kennzahlen für die Beurteilung des Sicherheitsabstandes zu einer bestandsgefährdenden Entwicklung aufzeigt,
- Festlegung von Schwellenwerten für Kennzahlen des Risikotragfähigkeitskonzepts, ab dem die Geschäftsleitung zu geeigneten Gegenmaßnahmen (s. § 1 StaRUG) und einer Information des Überwachungsorgans verpflichtet ist (z. B. bezüglich Insolvenzwahrscheinlichkeit oder Wahrscheinlichkeit einer bestandsgefährdenden Entwicklung (Gefährdungswahrscheinlichkeit)),
- 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.

6.4 Risikoidentifikation und -erfassung

51 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.

52 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.

53 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 müssen dabei die strategischen Risiken finden, 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 seltenen Extremrisiken (oder Kombinationseffekten von Risiken) ab, weshalb deren frühzeitige Erkennung wichtig ist.

54 Die Risikoidentifikation sollte eine systematische Beobachtung von Emerging Risks (neuartige, sich entwickelnde Risiken) umfassen. Gerade für die Früherkennung gem. § 91 Abs. 2 AktG sind Methoden zur Erkennung von Emerging Risks (z. B. Horizon Scanning, Weak Signal Analysis) relevant.

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

56 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 ent-

sprechend angepasst wird. Die Interne Revision untersucht, ob das Risikomanagementsystem alle wesentlichen Risiken erfasst, auch die Risiken infolge von Entscheidungen der Geschäftsleitung.

57 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.

58 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.

6.5 Risikoanalyse und -bewertung

59 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.

60 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.

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

62 Die Risikotragfähigkeit kann über eine Abschätzung der maximalen Risikowirkung (z. B. in Euro), die eine Organisation überstehen kann, und die Wahrscheinlichkeit für das Eintreten einer bestandsgefährdenden Entwicklung (Gefährdungswahrscheinlichkeit) gemessen werden. Die Gefährdungswahrscheinlichkeit ergibt sich aus der Risikoaggregation.

63 Damit wird die Risikotragfähigkeit über das wirtschaftliche Eigenkapital erfasst, das als Haftungsmasse zur Vermeidung einer Überschuldung zur Verfügung steht. Da Insolvenzen in der Regel durch Zahlungsunfähigkeit ausgelöst werden, sind weitergehende Risikotragfähigkeitskonzepte notwendig. Dabei sollte insbesondere geprüft werden, ob sich durch die Verletzung von Mindestanforderungen an das Rating oder Covenants eine (drohende) Illiquidität ergeben könnte.

64 Zu den Kennzahlen für die Messung der Risikotragfähigkeit sind Schwellenwerte anzugeben, bei deren Überschreiten die Geschäftsleitung geeignete Gegenmaßnahmen der Krisenabwehr initiieren und die Überwachungsorgane informieren muss. Die Entscheidung über solche Gegenmaßnahmen ist als unternehmerische Entscheidung aufzufassen und die Wirksamkeit für die Reduzierung des Risikoumfangs und damit der Gefährdungslage ist zu belegen (s. § 14 StaRUG).

65 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.

66 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.

67 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.

68 Die Risikoquantifizierung ist die Beschreibung von Risiken mittels einer geeigneten Dichte- oder Verteilungsfunktion, mit historischen Daten (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 mehrerer 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).

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

70 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. Die Aggregation der Risiken soll dabei unter Bezugnahme auf die Unternehmensplanung erfolgen, um aus der Planungslogik resultierende Abhängigkeiten der Risiken und das Risikodeckungspotenzial des Unternehmens sachgerecht zu berücksichtigen.

71 Außerdem ist das Risikobewertungssystem im Rahmen der Prüfung zu beurteilen. Dazu gehören

- die Festlegung geeigneter Risikostufen in Abhängigkeit von der Risikostrategie,
- die angemessene Darstellung der Interdependenzen zwischen Risiken und ihr Bezug zur Unternehmensplanung,
- die korrekte Durchführung der Aggregation von Risiken,
- die Ableitung eines Gesamtrisikos (z. B. Insolvenzwahrscheinlichkeit oder Gefährdungswahrscheinlichkeit als Ausdruck des Grads der Bestandsgefährdung),
- die Aktualität von Risikobewertungen.

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

6.6 Risikosteuerung und -überwachung

72 Gemäß dem Three Lines Model 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.

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

74 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. Ist ein solcher überschritten, sind geeignete Gegenmaßnahmen bis hin zu einer Restrukturierungsplanung zu initiieren (s. § 1 StaRUG).

75 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. (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?)

6.7 Risikoberichterstattung und -kommunikation

76 Das wesentliche Ziel der Risikoberichterstattung und Risikokommunikation ist es, den Entscheidungsträgern und Aufsichtsorganen zeitnah die Risikolage der Organisation widerzuspiegeln. Dabei muss über den Gesamtrisikoumfang und die Wahrscheinlichkeit einer bestandsgefährdenden Entwicklung informiert werden. Es sind sowohl regelmäßige Berichte als auch Ad-hoc-Risikomeldungen im konkreten Fall zu erstellen. Insbesondere ist sicherzustellen, dass bei der Vorbereitung wesentlicher Entscheidungen die Risikoinformationen für diese Entscheidungen zur Verfügung stehen. Außerdem sind externe Berichtspflichten, insbesondere zur Nachhaltigkeit nach CSRD/ESRS und den dort genannten Anforderungen an die Risikobewertung wesentlicher Nachhaltigkeitsrisiken, zu beachten.

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

78 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.

79 Für Aufsichtsräte ist die Risikoberichterstattung ein wichtiges Instrument im Rahmen der Erfüllung ihrer gesetzlichen Überwachungspflicht, die auch die Wirksamkeit des Risikomanagementsystems zum Inhalt hat. Aufsichtsräte sind bei einem kritischen Grad der Bestandsgefährdung, der geeignete Gegenmaßnahmen erfordert, über die Situation und die geplanten Gegenmaßnahmen durch die Geschäftsleitung zu informieren (§ 1 StaRUG).

80 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.

81 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.

7 Prüfung unternehmerischer Entscheidungen unter Risiko

82 Bei bedeutenden unternehmerischen Entscheidungen (z. B. Investitionen) fordert der Gesetzgeber (§ 93 Abs. 1 Satz 2 AktG), dass das Leitungsorgan auf Basis angemessener Informationen handelt, damit im Falle eines Schadeneintritts die Business Judgement Rule greifen kann und das Leitungsorgan nicht mangels Pflichtverletzung persönlich haftet. Die Business Judgement Rule ergibt sich richterrechtlich und teleologisch auch aus § 43 Abs. 1 GmbHG. Bei unternehmerischen Entscheidungen müssen nachweisbar angemessene Informationen vorliegen. Dazu gehören insbesondere die Informationen über die mit der Entscheidung verbundenen Risiken. Die frühzeitige Erkennung möglicher bestandsgefährdender Entwicklungen, die sich aus Kombinationseffekten von Risiken ergeben, ist nur möglich, wenn die mit einer unternehmerischen Entscheidung verbundene Veränderung des Gesamtrisikoumfangs des Unternehmens betrachtet wird. (Siehe ergänzend zu den Aufgaben des Risikomanagements bei der Vorbereitung bedeutender unternehmerischer Entscheidungen Tz. 21.)

83 Zu den bedeutenden unternehmerischen Entscheidungen im Sinne dieses DIIR-Revisionsstandards sind nur strategische und nicht operative oder taktische Entscheidungen zu rechnen. Dabei geht es nur um Entscheidungen der Leitungsorgane (Vorstand, Geschäftsführung), nicht des Managements.²

84 Die Legalitätspflicht ist zu beachten. Bei der Beachtung von Compliance-Vorgaben besteht grundsätzlich kein Entscheidungsspielraum (gebundene Entscheidung). Solche Entscheidungen sind daher nicht Gegenstand dieses DIIR-Revisionsstandards.

85 Bei der Prüfung der Vorbereitung unternehmerischer Entscheidungen ist zu unterscheiden zwischen der Prüfung des Managementsystems (Prozessprüfung, Systemprüfung) und der Prüfung von konkreten Entscheidungsvorlagen (stichprobenartig im Rahmen der Systemprüfung oder als Einzelfallprüfung). Die Interne Revision sollte prüfen, ob die

² Unternehmerische Entscheidungen betreffen strategische und langfristige Ziele des Unternehmens, während operative Entscheidungen kurzfristige Handlungen zur Umsetzung dieser Strategie betreffen. Sie haben meist weitreichende oder langfristige Auswirkungen auf das Unternehmen. Sie sind oft mit hohem Kapital- oder Ressourcenaufwand verbunden. Unternehmerische Entscheidungen werden typischerweise von der Unternehmensleitung getroffen. Beispiele: Wahl neuer Geschäftsfelder oder Expansion in internationale Märkte, Investition in große Produktionsanlagen oder neue Technologien, Entscheidung über Fusionen, Übernahmen oder Kooperationen, Einführung neuer Produktlinien oder Geschäftsmodelle, grundlegende Anpassung der Unternehmensstrategie zur Marktpositionierung.

Prozesse grundsätzlich belegbar eine adäquate Vorbereitung unternehmerischer Entscheidungen gewährleisten und einzeln betrachtete Entscheidungsvorlagen für unternehmerische Entscheidungen die maßgeblichen Kernanforderungen der Business Judgement Rule erfüllen. Die konkreten Anforderungen an die Fundierung einer Entscheidungsvorlage durch Informationen ergeben sich aus der Tragweite der Entscheidung für das Unternehmen.

86 Die Anforderungen an die Prozesse zur Vorbereitung unternehmerischer Entscheidungen im Sinne von § 93 Abs. 1 Satz 2 AktG und § 43 Abs. 1 GmbHG sind besonders hoch, weil die Beweislast für sachgerecht vorbereitete Entscheidungen und das Vorliegen angemessener Informationen nach § 93 Abs. 2 Satz 2 AktG bei der Geschäftsleitung liegt. Es sollte daher Gegenstand der Prüfung sein, ob eine Nachweisführung im Konfliktfall möglich wäre. Insbesondere ist darauf zu achten, dass die Entscheidungsvorlage vollständig, nachvollziehbar und frei von sachwidrigen Verzerrungen ist. Zum Beispiel kann der Prozess vorsehen, dass die Entscheidungsvorlage von einer neutralen, nicht vom Antragsteller abhängigen Funktion verantwortet wird, oder dass sie einer unabhängigen Qualitätssicherung unterliegt.

87 Die Prozesse müssen zentrale Aspekte hinsichtlich Struktur und Organisation enthalten. Typische Entscheidungen durchlaufen die in Abbildung 2 dargestellten Teilprozesse.



Abb. 2: Phasen des Entscheidungsprozesses

88 Im Rahmen der Prüfung von Entscheidungsvorlagen oder Entscheidungsprozessen sind zunächst ggf. extern bestehende Vorgaben und interne Richtlinien oder Handlungsempfehlungen durch eine Prozess-/Systemaufnahme zu erheben und durch Walk-Throughs zu validieren.

89 In der ersten Phase der **Feststellung des Entscheidungsbedarfs** ist zunächst zu klären, ob im Unternehmen eine eindeutige Begriffsdefinition der unternehmerischen Entscheidung hinsichtlich einer Abgrenzung gegen sonstige Entscheidungen existiert. Darüber hinaus sollten sinnvolle Verantwortlichkeiten und eine Bewertungsmethode festgelegt sein.

90 In der Phase der **Informationsgewinnung** geht es um die Identifikation und Beschaffung relevanter Informationen und Daten. Der Aufwand zur Entscheidungsvorbereitung muss in angemessenem Verhältnis zur Wesentlichkeit der Entscheidung stehen. Verantwortliche Stellen müssen in adäquater Weise in die Vorbereitung unternehmerischer Entscheidungen involviert sein. Neben einer unmittelbaren Mitwirkung des Risikomanagements ist es auch möglich, dass nach Vorgaben und Methoden des Risikomanagements Risikoanalysen durch andere Funktionen (z. B. Controlling oder M&A) vorgenommen werden. In diesen Fällen ist durch die Interne Revision zu prüfen, ob nach den Vorgaben des Risikomanagements gearbeitet wird und das Risikomanagement in der Lage ist zu beurteilen, ob die mit einer Entscheidung verbundenen zusätzlichen Risiken zu einem kritischen Anstieg des Grads der Bestandsgefährdung (§1 StaRUG) führen würden.

91 In der Phase der **Identifizierung von Alternativen** geht es vor allem um die Beurteilung, ob ausreichende und vollumfängliche Informationen zu Alternativen vorliegen. Entscheidend für die Vorbereitung der Entscheidung ist ein angemessener **Vergleich der Alternativen**. Es ist zu prüfen, ob klare Entscheidungskriterien und eine Bewertungsmatrix vorliegen.

92 In der Phase der **Entscheidung/Auswahl einer Alternative** ist zu klären, ob Vorgaben zu den zentralen Inhalten von Entscheidungsvorlagen existieren. Die Fundierung durch Informationen muss angemessen sein, d. h., der Aufwand für die Erstellung der Entscheidungsvorlage inklusive der Risikoanalyse steht in einem vertretbaren Verhältnis zu Risikogehalt und Investitionsvolumen.

93 Ergänzend könnte der Revisionsauftrag auch die Prüfung der sachgerechten **Umsetzung der Entscheidung** beinhalten. Dazu gehört die Überprüfung, ob die in der Entscheidungsvorlage genannten Risiken nach der Entscheidung in das operative Risikomanagementsystem überführt werden. Bei Entscheidungen, die im Rahmen von Projekten umgesetzt werden, sollte die Prüfung dem DIIR-Revisionsstandard Nr. 4 folgen. Dabei kann der Auftrag auch die **Überprüfung der Entscheidung** und des Entscheidungsprozesses im Sinne eines kontinuierlichen Verbesserungsprozesses umfassen.

94 Der ergänzende Prüfungsleitfaden zu unternehmerischen Entscheidungen kann als Hilfestellung für die Interne Revision bei der Prüfung einer einzelnen Entscheidung genutzt werden. Er kann aber auch bei der Systemprüfung des Prozesses für unternehmerische Entscheidungen hilfreich sein.

95 Der **Revisionsauftrag** ist wie immer im Vorfeld ausführlich mit dem Auftraggeber zu klären.

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 August 2026 auf www.diir.de

Version 2.2