

Deutsches Institut für Interne Revision (IIR)

IIR Revisionsstandard Nr. 2

**Prüfung des
Risikomanagement
durch die Interne Revision**

Ziel der Verlautbarung ist die Definition von Grundsätzen für die Prüfung des Risikomanagementsystems durch die Interne Revision. Diese Verlautbarung bezieht sich auf Unternehmen jeglicher Größenordnung in den Bereichen Industrie und Handel.

Interne Revision und Risikomanagement

- 1 **R i s i k o m a n a g e m e n t** ist ein nachvollziehbares, alle Unternehmensaktivitäten umfassendes Regelungssystem, das auf Basis einer definierten Risikostrategie ein systematisches und permanentes Vorgehen mit folgenden Elementen umfasst: Identifikation, Analyse, Bewertung, Steuerung, Dokumentation und Kommunikation sowie die Überwachung dieser Aktivitäten. Risikomanagement ist integraler Bestandteil der Geschäftsprozesse sowie der Planungs- und Kontrollprozesse.

- 2 Der Vorstand einer Aktiengesellschaft hat nach § 91 Abs. 2 AktG geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden (Risikomanagement- bzw. Risikofrüherkennungssystem). Die Vorschrift des § 91 Abs. 2 AktG gilt nach der sog. Ausstrahlungswirkung auch für die Vorstände/Geschäftsführungen/Geschäftsleitungen von Unternehmen in anderen Rechtsformen. Nach der Regierungsbegründung sollen durch diese Vorschrift die Verpflichtung des Vorstands, für ein angemessenes Risikomanagement und eine angemessene **I n t e r n e R e v i s i o n** zu sorgen, verdeutlicht werden. Mit dem Hinweis auf die Interne Revision wird deren Bedeutung hervorgehoben.

- 3 Das **R i s i k o m a n a g e m e n t s y s t e m** bzw. das Risikofrüherkennungssystem setzt sich aus folgenden Elementen zusammen:
 - **I n t e r n e s Ü b e r w a c h u n g s s y s t e m** mit organisatorischen Sicherungsmaßnahmen, internen Kontrollen und **I n t e r n e r R e v i s i o n**.
 - **C o n t r o l l i n g** (als Grundlage für eine zielgerichtete Steuerung des Unternehmens) mit den Subsystemen Planungssystem, Informationssystem, Kontrollsystem und Steuerungssystem (sog. Aktivitäten-Viereck) einschließlich Dokumentationssystem und Reportingsystem.
 - **R i s i k o m a n a g e m e n t s y s t e m** im engeren Sinne mit Risikostrategie, Risikomanagementprozess und Risiko-Controlling.

- 4 Da die Gesetzesbegründung Risikomanagement und Interne Revision nebeneinander stellt, aber nicht die Beziehung zueinander *expressis verbis* formuliert, kann weder aus dem Gesetz noch aus der Gesetzesbegründung unmittelbar abgeleitet werden, dass die Interne Revision das Risikomanagementsystem grundsätzlich prüfen muss. Es bleibt dem *Vorstand* im Rahmen seiner *allgemeinen Verantwortung* entsprechend § 76 AktG überlassen, in welcher Weise er absichert, dass das Risikomanagementsystem seine Aufgaben erfüllt.

Prüfung des Risikomanagementsystems durch die Interne Revision und durch den Abschlussprüfer

- 5 Es ist davon auszugehen, dass zumindest in *Größunternehmen* die notwendige Überwachung des Risikomanagementsystems ohne eine leistungsfähige Interne Revision nicht sichergestellt werden kann und der Internen Revision auf Grund ihrer allgemeinen Aufgabenstellungen sowie ihrer neutralen Position auch die unternehmensinterne Überwachung der Funktionsfähigkeit der Risikomanagementsysteme zu übertragen ist.

Sollte aufgrund der Größe und/oder der Struktur eines Unternehmens keine interne Revisionsfunktion vorhanden sein, hat die *Geschäftsleitung* in geeigneter Weise die Prüfung des Risikomanagements sicherzustellen.

- 6 Die *Interne Revision* als Bestandteil des Internen Überwachungssystems hat u.a. die *Aufgabe*, Mängel festzustellen und geeignete Verbesserungsmaßnahmen zu empfehlen sowie deren Umsetzung zu überwachen.

Die *Interne Revision* kann wie bisher schon bei der Einführung neuer Systeme bereits bei der Konzeption und Einführung des Risikomanagementsystems beratend tätig sein. Die laufende Verantwortung für die Durchführung des Risikomanagementsystems kann aber wegen des bestehenden Interessenkonfliktes nicht der Internen Revision übertragen werden.

- 7 Der *Abschlussprüfer* hat bei einer Aktiengesellschaft, die Aktien mit einer amtlichen Notierung ausgegeben hat, im Rahmen der Prüfung zu beurteilen, ob der Vorstand die ihm nach § 91 Abs. 2 des Aktiengesetzes obliegenden Maßnahmen in einer geeigneten Form getroffen hat und ob das danach einzurichtende Überwachungssystem seine

Aufgaben erfüllen kann (§ 317 Abs. 4 HGB). Der Abschlussprüfer hat außerdem zu beurteilen, ob die zur Einrichtung eines Überwachungssystems getroffenen Maßnahmen während des gesamten zu prüfenden Zeitraums eingehalten wurden. Der Abschlussprüfer hat das Ergebnis seiner Prüfung nach § 317 Abs. 4 HGB in einem besonderen Teil des Prüfungsberichts darzustellen. Es ist darauf einzugehen, ob Maßnahmen erforderlich sind, um das Interne Überwachungssystem zu verbessern (§ 321 Abs. 4 HGB).

- 8 Im Prüfungsstandard IDW PS 340 Rz. 6 wird ausgeführt, dass die Reaktion des Vorstands auf erfasste und kommunizierte Risiken selbst nicht Gegenstand der Maßnahmen i.S.d. § 91 Abs. 2 AktG und damit auch nicht Gegenstand der Prüfung nach § 317 Abs. 4 HGB ist. Ebenso gehört die Beurteilung, ob die von nachgeordneten Entscheidungsträgern eingeleiteten oder durchgeführten Handlungen zur Risikobewältigung bzw. der Verzicht auf solche sachgerecht oder wirtschaftlich sinnvoll sind, **n i c h t** zur Prüfung des Risikofrüherkennungssystems durch den Abschlussprüfer.
- 9 Der Umfang der **Z u s a m m e n a r b e i t v o n I n t e r n e r R e v i s i o n** und **A b s c h l u s s p r ü f e r** wird wesentlich dadurch bestimmt, dass die Beurteilung der Eignung der Maßnahmen nach § 91 Abs. 2 AktG durch den Abschlussprüfer auch eine Prüfung voraussetzt, ob das eingerichtete Interne Überwachungssystem – also die organisatorischen Sicherungsmaßnahmen, die integrierten Kontrollmaßnahmen und die Prüfungstätigkeit der Internen Revision – ausreicht, um die Funktionsfähigkeit des Systems zu gewährleisten.

Der Abschlussprüfer muss schon im Interesse der Wirtschaftlichkeit der Prüfungsdurchführung auf die Ergebnisse der Prüfungstätigkeit der Internen Revision zurückgreifen. Ebenso sollte die Interne Revision sich bei eigenen Prüfungshandlungen auf die Ergebnisse des Abschlussprüfers stützen. Durch die Absprache der Prüfungstätigkeiten kann deren Effizienz gesteigert werden. Dabei ist zu berücksichtigen, dass der Aufsichtsrat in der Regel der Auftraggeber des Abschlussprüfers ist, Auftraggeber der Internen Revision aber der Vorstand/die Geschäftsleitung.

- 10 Im Übrigen wird auf den **I I R R e v i s i o n s s t a n d a r d N r . 1** „Zusammenarbeit von Interner Revision und Abschlussprüfer“ verwiesen.

Ausgangspunkt, Ziel und Umfang der Prüfung des Risikomanagementsystems im engeren Sinne durch die Interne Revision

- 11 Ausgangspunkt der Prüfung des Risikomanagementsystems ist die Risikomanagementsstrategie. Hierbei ist insbesondere sicherzustellen, dass das Risikomanagement von der Unternehmensleitung als Teil der Corporate Governance gesehen wird und ein entsprechender Beschluss der Unternehmensleitung hinsichtlich der Einrichtung und laufenden Anwendung eines Risikomanagementsystems existiert.
- 12 Die Interne Revision hat festzustellen,
 - ob ein fundiertes, von der Unternehmensleitung getragenes und dokumentiertes Risikomanagementsystem existiert,
 - ob die tatsächlichen Abläufe dem definierten System entsprechen, ob also der Risikomanagementprozess umfassend und kontinuierlich durchgeführt wird und ob die Ergebnisse in geeigneter Weise dokumentiert und kommuniziert werden,
 - ob die festgelegten Maßnahmen tatsächlich umgesetzt wurden.
- 1 Darüber hinaus ist die Risikoidentifikation, die Risikobewertung und die Zweckmäßigkeit der Maßnahmen inhaltlich zu beurteilen.
- 14 Intensität und Häufigkeit der Prüfungen sind u.a. in Abhängigkeit von der Komplexität der Wertschöpfung, Unternehmensgröße und Dynamik der Unternehmensentwicklung festzulegen.

Prüfung der Konzeption und der Organisation des Risikomanagementsystems

- 15 Es ist zu untersuchen, ob eine klare **Konzeptbeschreibung** und ob eindeutige **Regelungen** hinsichtlich Zuständigkeiten und Dokumentation für alle Unternehmensebenen vorliegen.
- 16 Im Einzelnen sind folgende die **Organisation**, **Verantwortlichkeit** und **Dokumentation** betreffende Punkte ggf. mittels einer Checkliste zu untersuchen:
- Ist ein Riskmanager (und/oder andere Stelle oder Funktion im Unternehmen) eingesetzt, der für Koordination und Unterstützung hinsichtlich des Risikomanagements verantwortlich ist ?
 - Gibt es eine Organisations-Richtlinie, ein Handbuch oder Arbeitsanweisungen, in denen die organisatorischen Regelungen und Maßnahmen des Risikomanagementsystems einschließlich der Implementierung und der Durchführung geregelt sind ?
 - Ist im Unternehmen geregelt, dass die Verantwortung für ein funktionierendes Risikomanagementsystem bei den Geschäfts-/Organisationseinheiten liegt ?
 - Wurden adäquate Wesentlichkeitskriterien (z.B. in Form von Schwellenwerten) hinsichtlich der Risikozuordnung zu verantwortlichen Bereichen definiert ?
 - Ist die Identifizierung der Risiken unter Verantwortung des Top-Managements des jeweiligen Geschäftsbereiches erfolgt und liegt eine entsprechende Dokumentation vor ?
 - Wird die Risikolage des Unternehmens im Rahmen einer vorgegebenen Systematik regelmäßig mindestens jährlich auf Aktualität geprüft ?
 - Ist die Risikobeschreibung ausreichend detailliert ?

- Ist sichergestellt, dass bei plötzlichen und unvorhergesehenen Veränderungen in der Risikolandschaft des Unternehmens eine Aktualisierung der Risiken hinsichtlich Organisation, Verantwortlichkeit und Dokumentation in angemessenen Zeitabständen erfolgt ?
- Werden Risiken mit gleicher Ursache kumuliert ?

Prüfung der vollständigen Erfassung und der Identifikation aller Risiken

- 17 Es muss sichergestellt sein, dass das Risikomanagementsystem alle wesentlichen Risiken erfasst, wobei auch die in die Zukunft reichenden strategischen Entscheidungen mit den dazugehörenden Risiken zu betrachten sind.
- 18 Die Risikoidentifikation hat alle Gesellschaften/Betriebsstätten, Geschäftsbereiche und Geschäftsfelder eines Unternehmens im Inland und im Ausland, von denen wesentliche Risiken ausgehen können, zu erfassen. Dabei sind neben den Kerngeschäftsprozessen (z.B. Forschung und Entwicklung, Einkauf, Produktion, Marketing und Vertrieb, Kundendienst) auch die Unterstützungsprozesse (z.B. Finanzen, Personal, Informationstechnologie, Logistik) einzubeziehen. Kompetenzschnittstellen zwischen dezentralen Geschäftseinheiten und Zentralfunktionen sind ggf. zu analysieren.
- 19 Zur Prüfung der Vollständigkeit der Risikoidentifikation sollten geeignete Checklisten verwendet werden.

20 Tab.: Übersicht möglicher Risikofelder

Risikofelder	Trifft zu	Eingeschränkt	Trifft nicht zu
Externe Risiken			
Verhalten der Wettbewerber			
Marktrisiko (Mengen-/Preisrisiko)			
Branchen- und Produktentwicklung			
Besteuerung/Betriebsprüfungen			
Politische und rechtliche Entwicklung			
Umweltkatastrophen/Krieg			
Strategische Risiken			
Beteiligungen			
Produkt			
Investitionen			
Standort			
Informationsmanagement			
Länderrisiken			
Operative Risiken			
Produkte			
Fertigung			
Produktivität			
Kapazität			
Kunden			
Lieferanten			
Lagerhaltung			
Logistik			
Umweltmanagement			
Warenzeichen/Patente			
Öffentlich-rechtliche Genehmigungen			
Gewährleistung/Haftungsrisiken			
Personengefährdung/Arbeitsschutz			
Steuerungssysteme			
Kontrollsysteme			
Investitionen/Ersatzbeschaffungen			
Personalrisiken			
Management Nachfolgeregelung			
Qualifikation			
Integrität und dolose Handlungen			
Fluktuation			
Datenverarbeitung			
Systemlogik			
Zugriff			
Verfügbarkeit (Ausfall/Datenverlust)			
Lizenzmissbrauch Software			

Finanzwirtschaftliche Risiken			
Liquidität			
Wechselkursrisiken			
Zinsänderungsrisiken			
Wertpapierkursrisiken			
Adressenausfallrisiken			
Kreditlinien			
Sonstige Risiken			
Corporate Governance			
...			

21 **B a s i s** für die Prüfung der Vollständigkeit :

- Dokumentation aus der Risikoidentifikation, z.B. Protokolle oder o.g. Checklisten für die Fragestellung, ob innerhalb der Kerngeschäftsprozesse bzw. Unterstützungsprozesse alle wesentlichen Risiken erfasst werden.
- Organisationspläne für die Fragestellung, ob alle wesentlichen Betriebsstätten, Geschäftsbereiche und Geschäftsfelder berücksichtigt werden.
- Anteilsbesitz gem. § 285 Nr. 11 HGB bzw. § 313 Abs. 4 HGB bzw. Prüfungsberichte der Wirtschaftsprüfer für die Fragestellung, ob alle wesentliche Tochtergesellschaften in die Risikoidentifikation einbezogen werden.

22 Die Prüfung der Vollständigkeit kann durch entsprechende **I n t e r v i e w s** der Revision mit den **V e r a n t w o r t l i c h e n** abgesichert werden.

Beurteilung der Risikoanalyse und der Risikobewertung

23 Zur Ableitung von angemessenen Steuerungsmaßnahmen bedarf es einer weiteren Analyse und Bewertung der identifizierten Risiken. Die Risiken sollen mit Hilfe der Risikoanalyse **q u a l i t a t i v b e u r t e i l t** und **q u a n t i t a t i v g e m e s s e n** werden. Die Risiken werden üblicherweise hinsichtlich der Höhe des potentiellen Schadens und dessen Eintrittswahrscheinlichkeit bewertet, und zwar zunächst hinsichtlich der **B r u t t o r i s i k e n** (vor Risikosteuerung/Sicherungsmaßnahmen).

- 24 Die Interne Revision soll bei der Beurteilung der Risikoanalyse und der Risikobewertung die entsprechenden Bewertungen hinsichtlich Schadenshöhe und Eintrittswahrscheinlichkeit auf **Plausibilität des Bewertungssystems** und einzelne Bewertungsvorgänge **stichprobenartig** prüfen.

Kumulationen und **Interdependenzen** sind zu beachten.

- 25 Die **Aktualität** der Bewertung stellt einen weiteren Aspekt der Prüfungstätigkeit dar.

Prüfung der Realisierung und Zweckmäßigkeit der Maßnahmen zur Risikosteuerung und der Einhaltung der integrierten Kontrollen

- 26 Die bei der Risikoidentifikation und Risikoanalyse ermittelten Risikopositionen sollen im Rahmen der **Risikosteuerung** aktiv beeinflusst werden. Die Steuerungsmaßnahmen zielen dabei auf die Verringerung der Eintrittswahrscheinlichkeit, z.B. durch Kontrollen, oder auf eine Begrenzung der Risikoauswirkungen, z.B. durch Versicherungen, ab.

- 27 Durch die Prüfung der Internen Revision soll festgestellt werden, ob die vorgegebenen Maßnahmen auch tatsächlich kontinuierlich umgesetzt werden. Außerdem ist die Zweckmäßigkeit der Maßnahmen zu beurteilen. Dabei ist es erforderlich, die **Abwägung von Chancen und Risiken** in die Prüfung einzubeziehen. Schließlich muss festgestellt werden, ob die integrierten Kontrollen (z.B. Funktionstrennungen, Limit- und Kompetenzregelungen, Vier-Augen-Prinzip) tatsächlich eingehalten werden.

- 28 Die folgenden **Fragen** müssen durch die Interne Revision beantwortet werden:

- Gibt es Frühindikatoren, geeignete Meldewege und eindeutig definierte Eingreifkriterien ?
- Ist geregelt, wer für die erforderlichen Maßnahmen verantwortlich ist ?
- Wird die Angemessenheit der Maßnahmen vor dem Hintergrund des sich wandelnden Umfelds regelmäßig hinterfragt ?

- Liegt eine angemessene Dokumentation vor, anhand der eine Überprüfung der Maßnahmen erfolgen kann ?

Prüfung der Kommunikation von Risiken

- 29 Die frühzeitige empfängerorientierte Kommunikation über wesentliche Risiken ist von zentraler Bedeutung für die Funktionsfähigkeit des Risikomanagements. Nach Bewertung der Restrisiken (**N e t t o r i s i k e n**) sollte durch Festlegung von **W e s e n t l i c h - k e i t s g r e n z e n** für jede Berichtsebene definiert werden, welche Risiken in welchen Zeitabständen an die zuständigen Entscheidungsträger zu berichten sind. Dabei muss sichergestellt sein, dass bestandsgefährdende Risiken oder Risiken mit wesentlicher Auswirkung auf die Vermögens-, Finanz- und Ertragslage umgehend und direkt dem Vorstand/der Geschäftsführung zugeleitet werden, u.a. für die börsengesetzliche **A d - h o c - B e r i c h t e r s t a t t u n g** .
- 30 Die Interne Revision prüft, ob die festgelegten **I n f o r m a t i o n s f l ü s s e** und **R e g e l u n g e n** zur Berichterstattung eingehalten werden, insbesondere hinsichtlich Vollständigkeit, Zeitnähe, Verantwortlichkeiten und Verständlichkeit.