Hinweise zur Prüfung des Risikomanagement-systems

Praxisleitfaden zum DIIR Revisionsstandard Nr. 2

Fachgruppe Risikomanagement des DIIR-Arbeitskreises „Interne Revision im Mittelstand“

DIIR Deutsches Institut für Interne Revision e.V.

Inhalt

Abkürzungsverzeichnis

Abs.	Absatz
Abschn.	Abschnitt
AG	Aktiengesellschaft
AktG	Aktiengesetz
bzw.	beziehungsweise
COSO	Committee of Sponsoring Organizations of the Treadway Commission
COSO-ERM	COSO-Enterprise Risk Management Framework
DIIR	Deutsches Institut für Interne Revision e.V.
DIN	Deutsche Industrienorm
ERM	Enterprise Risk Management
etc.	et cetera (und so weiter)
FMEA	Failure Mode and Effects Analysis/Fehler-Möglichkeits- und Einfluss-Analyse
ggf.	gegebenenfalls
ggü.	gegenüber
GmbH	Gesellschaft mit beschränkter Haftung
GmbHG	GmbH-Gesetz
IDW	Institut der Wirtschaftsprüfer in Deutschland e.V.
IDW PS	Prüfungsstandards des Instituts der Wirtschaftsprüfer
IIA	Institute of Internal Auditors
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
o. a.	oben angegeben
o. ä.	oder ähnlich
PS	Prüfungsstandard
Tz.	Textziffer
u. a.	unter anderem
z. B.	zum Beispiel

1 Präambel

Die Entwicklung des Risikomanagements sowohl in den Unternehmen als auch in der einschlägigen Literatur in den letzten Jahren kann mit Fug und Recht als dynamisch bezeichnet werden. Längst handelt es sich nicht mehr um eine intellektuelle Fingerübung, die in Großunternehmen für gut ausgestattete Stabsbereiche als sekundäre Aufgabe anfiel.

Vielmehr wird heute bis in mittelständische Strukturen risikoorientiert gedacht und das Geflecht von Vertretung des Unternehmens gegenüber den Stakeholdern, den Finanzmärkten und den Aufsichtsbehörden mit Methoden des Risikomanagements angegangen.

Hier ist die Interne Revision gefragt, ihren Auftrag gegenüber der Unternehmensleitung wahrzunehmen und durch eine qualitativ hochwertige Prüfung dieses noch relativ jungen Managementgebietes zur „Assurance“ im Unternehmen beizutragen.

Zu diesem Zweck wurde der vorliegende Praxisleitfaden als Hilfe von Mitgliedern der Fachgruppe „Risikomanagement“ des Arbeitskreises „Interne Revision im Mittelstand“ des DIIR – Deutsches Institut für Interne Revision e.V. erstellt.

Er soll den DIIR Revisionsstandard Nr. 2 „Prüfung des Risikomanagementsystems durch die Interne Revision“ ergänzen. Dabei wurde von Seiten der Autoren besonderer Wert auf die Praxistauglichkeit auch in mittleren und kleineren Revisionseinheiten gelegt.

2 Adressaten, Verbindlichkeit und Geltungsbereich

In Bezug auf den DIIR Revisionsstandard richtet sich der Leitfaden an den Mittelstand – unabhängig von Branche und Rechtsform – und ist eine unverbindliche Praxishilfe für die Prüfungsdurchführung.

Bei der Prüfung des Risikomanagements kann je nach Unternehmen der Fragenkatalog individuell angepasst werden.

3 Grundlagen des Risikomanagements

Neben der Erfüllung der gesetzlichen und aufsichtsrechtlichen Vorgaben stellt ein eingerichtetes und funktionierendes Risikomanagement die nachhaltige Leistungsfähigkeit im Wettbewerb sicher. Das Ziel des Risikomanagements ist eine frühzeitige und systematische Erkennung, Analyse, Bewertung, Steuerung und Überwachung von Risiken.

Die Unternehmensleitung wird durch den Aufbau einer zuverlässigen Grundlage für die (risikobewusste) Entscheidungsfindung und Planung unterstützt. Dabei wird die Einhaltung relevanter gesetzlicher und regulatorischer Anforderungen, internationaler Normen sowie des Ordnungsrahmens für die Leitung und Überwachung des Unternehmens (Corporate Governance) sichergestellt.

Nach dem Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) gibt es eine rechtliche Verpflichtung zur Risikofrüherkennung, die einen Teilbereich des Risikomanagements darstellt.

Ergänzend zu der Sorgfaltspflicht seiner Leitungsaufgabe nach § 93 AktG ist das Unternehmen nach § 91 Abs. 2 AktG verpflichtet „geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden“. Die Regierungsbegründung BT Drucksache 13/9712 erweitert die Ausstrahlungswirkung dieses Gesetzes auch auf Organisationen anderer Rechtsformen.

Das Risikofrüherkennungssystem ist zudem Gegenstand der gesetzlichen Jahresabschlussprüfung durch den Abschlussprüfer. Im Rahmen dessen wird das System gemäß § 317 Abs. 4 HGB sowie IDW Prüfungsstandard 340 auf das Vorhandensein, die kontinuierliche Wirksamkeit sowie seine Eignung hin überprüft, unternehmensgefährdende Risiken und Entwicklungen frühzeitig zu erkennen. Ob das Unternehmen den Risiken effektiv und effizient entgegengetreten ist, ist in der Regel nicht Prüfungsgegenstand der gesetzlichen Abschlussprüfung, sondern einer Internen Revision.

Gesetzliche Grundlage des Risikomanagements für den öffentlich-rechtlichen Sektor ist der § 53 des Haushaltsgrundsätzegesetzes (HGrG), der seine Entsprechung im Prüfungsstandard 720 des IDW findet.

Derzeit existieren weltweit über 80 Rahmenwerke und Normen zu Risikomanagement, z. B. COSO Enterprise Risk Management Framework (COSO ERM oder COSO II), ISO 31000: Guidelines for principles and implementation of risk management, ONR 49000: Risikomanagement für Organisationen und Systeme, DRS 5: Risikoberichterstattung, IDW PS 340 etc.

Im Hinblick auf die Anwendung von Rahmenkonzepten für ein Risikomanagement gibt es bislang keine gesetzlichen Vorschriften, sich zwingend an Standards zu orientieren. Dennoch sichern diese eine strukturierte Vorgehensweise und werden von Prüfinstanzen begrüßt.

4 Begriffsdefinitionen

Dieser Praxisleitfaden orientiert sich an den Begriffsdefinitionen des DIIR Revisionsstandard Nr. 2.

Weiterführende Begriffsdefinitionen finden sich u. a. in der ISO 31000, der ONR 49000 und im Glossar des COSO ERM Integrated Framework.

5 Auftrag der Internen Revision zur Prüfung des Risikomanagementsystems

Aus den im Kapitel 3 dargestellten rechtlichen Grundlagen zur Einführung eines Überwachungs- und Risikofrüherkennungssystems leiten sich die Aufgaben der Internen Revision ab.

Im Einklang mit der Definition der Internen Revision durch das DIIR und durch das Institute of Internal Auditors sowie den „Internationalen Standards für die berufliche Praxis der Internen Revision“ geht der Auftrag hervor, die Funktionsfähigkeit der Risikomanagementprozesse zu beurteilen und zu deren Verbesserung beizutragen.

In Anlehnung an den „IIA Fächer“ zur Abgrenzung der Internen Revision vom Risikomanagement ist der rote Bereich, soweit im Mittelstand möglich, durch die Interne Revision auszugrenzen. Für den Fall, dass die Interne Revision in Personalunion das Risikomanagement mitbetreut, zeigt die folgende Abbildung den möglichen Handlungsspielraum auf:

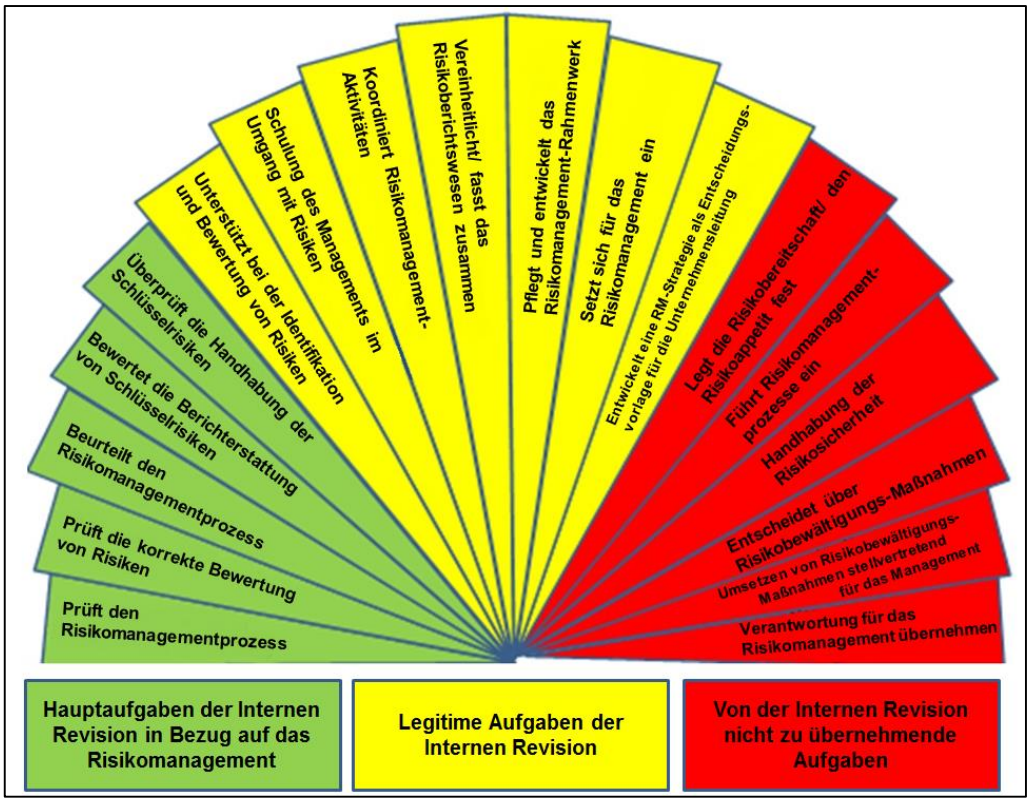

Abbildung: Aufgaben der Internen Revision in Bezug auf das Risikomanagement, Quelle: Institute of Internal Auditors – UK and Ireland Ltd: Position Statement: The Role of Internal Audit in Enterprise-wide Risk Management

6 Prüfung der Risikomanagementphasen

6.1 Risikomanagement-Organisation

Sollzustand:

Risikopolitische Grundsätze sind klar, eindeutig und verbindlich festgelegt. Die Risikomanagement-Organisation ist derart ausgestaltet, dass die Ziele effektiv und effizient erreicht werden können.

Verantwortlichkeiten, Aufgaben, Kompetenzen und Kommunikationswege sind definiert, bekannt und werden eingehalten.

Prüfung:

Interview mit Risikomanagement-Beteiligten aller Ebenen (Top Management, Risk Owner, Risikomanager), Einsichtnahme in vorhandene Dokumentationen (z. B. Risikomanagement-Handbücher etc.).

- Sind Auf- und Ablauforganisation des Risikomanagements definiert und angemessen?
- Sind entsprechende Dokumentationen angemessen, verständlich und korrekt?
- Werden definierte Vorgaben eingehalten?
- Ist die Gesamtverantwortung für das Risikomanagementsystem in der Geschäftsführung verankert?
- Wurden alle Aufgaben im Risikomanagement zielgerichtet definiert und kommuniziert?
- Wird Risikomanagement ausreichend in alle betrieblichen Verfahren und Prozesse integriert?
- Finden die Risikomanagementphasen in allen Teilen und auf allen Hierarchieebenen des Unternehmens statt?
- Wurden Vorgaben (z. B. Risikodefinition, Risikoappetit, Key Risk Indikatoren, organisatorische Regelungen etc.) ausreichend kommuniziert?
- Sind alle Risikomanagement-Beteiligten ausreichend geschult, um ihre Aufgaben wahrnehmen zu können?

- Wird das Funktionieren des Risikomanagements auch in Ausnahmefällen (z. B. Abwesenheit von Mitarbeitern, Ausfall technischer Systeme, erhöhte Belastung durch Sonderaufgaben) organisatorisch sichergestellt?
- Wird die Angemessenheit der organisatorischen Vorgaben für das Risikomanagement regelmäßig überwacht und, sofern notwendig, angepasst und weiter entwickelt?

6.2 Risikostrategie

Sollzustand:

Die Risikostrategie ist aus der Unternehmensstrategie abgeleitet, umfasst den Risikoappetit des Unternehmens und berücksichtigt die Risikotragfähigkeit.

Aus der Ausgestaltung der Risikostrategie kann die operative Steuerung der Risiken abgeleitet werden.

Prüfung:

- Wurden Risikostrategie und Risikoappetit definiert, dokumentiert und kommuniziert?
- Ist die Risikostrategie mit der Gesamtstrategie des Unternehmens konsistent?
- Können aus ihr operative Maßnahmen abgeleitet werden?
- Wird die Risikostrategie regelmäßig und anlassbezogen auf ihre Angemessenheit und Aktualität überprüft?
- Erfolgt eine adäquate Dokumentation und Kommunikation der Risikostrategie?

Weitere Prüfungsansätze zur Risikostrategie finden sich in Kapitel 6.2 des Revisionsstandards Nr. 2.

6.3 Risikoidentifikation und -erfassung

Sollzustand:

Alle wesentlichen Risiken (ggf. sind Meldeschwellen zu beachten) sollten in einem Inventar aufgeführt und aktuell sein.

Alle Geschäftseinheiten und organisatorischen Ebenen (inkl. In- und Ausland) sollten an der Risikoidentifikation beteiligt sein.

Prüfung:

Nach der allgemeinen Prüfung des Risikomanagementsystems sollte eine Prüfung zentral, in ausgewählten Geschäftseinheiten und organisatorischen Ebenen des Unternehmens stattfinden.

Hierbei bieten sich Interview mit dem entsprechenden Management an. Zur Identifikation geeigneter Geschäftseinheiten und organisatorischen Ebenen kann z. B. eine Stichprobenprüfung auf Basis von Organigrammen erfolgen.

Vollständigkeit:

Gibt es im Unternehmen ein einheitliches Verständnis von „Risiko“?

- Prüfung, ob es eine schriftliche und kommunizierte Definition im Unternehmen gibt. Interview mit Vertretern unterschiedlicher Bereiche, was diese unter einem Risiko verstehen.

Sind alle wesentlichen Betriebsstellen, Geschäftsbereiche, Geschäftsfelder, Prozesse z. B. Geschäftsführung, Controlling, Managementsysteme (Qualität, Umwelt, Informationssicherheit o. ä.) Personalwesen, Materialwirtschaft, Instandhaltung und Wartung etc. des Unternehmens in das Risikomanagement eingebunden?

- Erfolgt die Identifikation anhand der Wertschöpfungskette oder entlang der Funktionsbereiche? Ist die Unternehmensleitung mit eingebunden?
- Prüfung durch Interview mit dem entsprechenden Management. Hierzu z. B. Stichprobenprüfung auf Basis Organigramm oder Geschäftseinheiten und organisatorischen Ebenen, die im Inventar nicht auftreten („weiße Flecken“).

Lassen sich wesentliche Risiken aus den Aufgaben und Zielen des Unternehmens ableiten?

- Sind diese im Risikoinventar berücksichtigt? Falls nicht, kann dies begründet werden?
- Sichtung der dokumentierten, quantifizierten Unternehmensziele, Abgleich mit dem Risikoinventar, Interview mit den Verantwortlichen.

Wie wird die Identifikation aller wesentlichen Risiken sichergestellt?

- Interview mit den Verantwortlichen, Prüfung des Risikomanagement-Handbuchs, Abgleich mit dem Risikoinventar.

Wie werden Risiken in das Inventar aufgenommen?

Wenn Workshops stattfinden, wer sind die Teilnehmer?

- Nehmen z. B. das internationale Management bzw. Fachleute teil oder wird nur national beurteilt?
- Wenn Frage- oder Erfassungsbögen verwendet werden: Wie ist der Rücklauf und gibt es eine Ausgrenzung einzelner Bereiche?
- Erfolgt die Identifikation insgesamt in geeigneter und nachvollziehbarer Form?

Werden die richtigen Methoden richtig angewendet?

- Diese können z. B. sein: Brainstorming, Workshops, Morphologische Matrix, Delphi-Methode, strukturierte Interviews, Gesprächsleitfäden, Root Cause Analysis, Szenario-Technik, Gefährdungsanalysen, SWOT-Analyse, Markt- und Wettbewerbsanalyse, Lessons Learned etc.
- Prüfung z. B. eines vorliegenden Risikomanagement-Handbuchs des Unternehmens, Interview mit dem Risikomanagement, Sichtung Protokolle auf durchgeführte Methoden und Ergebnisse, Interview der Verantwortlichen, Sichtung von Protokollen und Risikoberichten, Abgleich mit dem Organigramm, Abgleich mit dem Risikoinventar.

Wurden die in die Zukunft reichenden strategischen Entscheidungen mit den dazugehörigen Risiken betrachtet?

- Interview mit den Verantwortlichen zur Unternehmensstrategie, Sichtung von vorhandenen Dokumentationen zur Strategie, Ableitung potentieller Risiken, Abgleich mit dem Risikoinventar.

Werden durch die Interne Revision, den Abschlussprüfer oder andere Prüfer festgestellte Risiken mit in das Risikoinventar aufgenommen?

- Dies können z. B. sein: stichprobenartiger Abgleich von in Revisionsberichten/andere Prüf-/Auditberichten/Managementlettern aufgeführten Risiken mit dem Risikoinventar.

Wie ist sichergestellt, dass Risikomeldungen vergleichbar sind? Gibt es einen formalen Prozess, Formulare, Leitfäden etc?

- Interview mit den Verantwortlichen, Sichtung des Risikomanagement-Handbuchs sowie vorhandener Formulare und Vorlagen.

Sind alle gemeldeten Risiken im Risikoinventar aufgeführt?

- Abgleich der Workshop-Ergebnisse (Protokolle etc.) und Fragebögen mit dem Inventar. Ggf. Ergänzung durch Interview mit dem Management.

Wie wird eine Vollständigkeit des Risikoinventars sichergestellt?

- Gibt es Risiken, die im Inventar fehlen? Falls ja, kann dies begründet werden?
- Gibt es Meldeschwellen, ab wann Risiken gemeldet werden müssen? Werden diese eingehalten?
- Abgleich möglicher Risiken/Musterliste (siehe Anhang) sowie z. B. weiterer Listen (z. B. Bundesamt für Sicherheit in der Informationstechnik, Polizeiliche Kriminalstatistik) mit dem Risikoinventar. Abgleich mit der Vorperiode.

Sind das politische sowie rechtliche Umfeld (Kontext) bei der Erstellung des Risikoinventars berücksichtigt?

- Interview mit den Verantwortlichen, Zusammenstellung einer Übersicht über das rechtliche Umfeld des Unternehmens, Abgleich mit der im Unternehmen vorhandenen Dokumentation, Prüfung, ob sich z. B. branchenspezifische Risiken im Risikoinventar widerfinden.

Handelt es sich um ein „Alibi-Risikomanagement“?

- Ist das Risikoinventar Thema z. B. in Geschäftsführungsprotokollen/Vorstandsprotokollen als besprochen aufgeführt oder z. B. vor der Einführung neuer Geschäftsfelder diskutiert?
- Sichtung der Protokolle, Interview mit den Verantwortlichen.

Wer ist für die Risikoidentifikation und -erfassung verantwortlich?

- Gibt es eine Dokumentation, die Verantwortlichkeiten fest zuteilt?
- Erfolgen die Identifikation und Erfassung zentral oder dezentral?
- Gibt es für eine dezentrale Erfassung beratende Ansprechpartner?
- Interview mit den Verantwortlichen, Sichtung des Risikomanagement-Handbuchs.

Wie werden Veränderungen der Risikolandschaft im Risikomanagement berücksichtigt?

- Interview mit den Verantwortlichen zur Veränderung des Unternehmensumfelds, Ableitung potentieller Risiken, Abgleich mit dem Risikoinventar.

Wie wird mit Doppelnennungen von Risiken durch unterschiedliche Bereiche umgegangen?

- Prüfung des Risikoinventars auf Doppelnennungen, Interview mit den Verantwortlichen.

Werden Risiken auf Konzern-/Gruppenebene konsolidiert?

- Prüfung der Dokumentation und Kommunikation auf Konzern-/Gruppenebene.

Werden Risiken, die eingetreten sind bzw. deren Eintritt gewiss ist und die in die Unternehmensplanung bereits eingestellt sind, nicht mehr im Risikoportfolio aufgeführt? Ist dies angemessen?

- Interview mit den Verantwortlichen, Prüfung des Risikomanagement-Handbuchs, Abgleich des Risikoinventars mit der Unternehmensplanung.

Wird die Risikoidentifikation im Ergebnis strukturiert in einem Risikoinventar dargestellt (Risikoregister, -katalog, -liste, -landkarte)?

Aktualität:

Wird Risikomanagement gelebt und akzeptiert?

- Werden die Risiken wirklich und zeitnah gemeldet?
- Werden unterjährig neu aufgetretene Risiken identifiziert und berichtet?
- Prüfung des Risikoinventars ggü. Interview mit verantwortlichen (lokalen) Managern. Abgleich Erfassungs-/Reporting-Zeitpunkt mit Zeitpunkt der Identifikation/Meldung.

Ist das Risikoinventar aktuell? Wie häufig erfolgt eine Aufnahme/Aktualisierung?

- Prüfung der Risikoberichte und des Risikomanagement-Handbuchs, Interview mit den Verantwortlichen.

Gibt es über Jahre gleichbleibende Risiken, obwohl sich z. B. das Geschäftsmodell/die Unternehmensstrategie oder das Unternehmensumfeld (rechtliche, gesetzliche, politische, technische Aspekte etc.) verändert haben?

- Prüfung der Risikoinventar-Historie, Vergleich der Risk-Reports, Interview mit dem Management.

Werden in der Vorperiode eingetretene Risiken analysiert (Lessons Learned)?

- Prüfung der Versicherungsfälle, des „Lost-Reportings“, der Rückstellungen und des Gewährleistungsbedarfs.

6.4 Risikoanalyse und -bewertung

Sollzustand:

Alle Risiken müssen nach einer strukturierten, vergleichbaren und einheitlichen Methode untersucht werden.

Der Charakter (z. B. Art des Auftretens, Ereignis oder Entwicklung) muss dabei erkennbar werden.

Risikoanalyse und -bewertung ermöglichen eine Priorisierung von Risiken und Steuerungsmaßnahmen durch ein geeignetes Risikomaß. Für alle Risiken des Risikoinventars sind die Eintrittswahrscheinlichkeit und Auswirkung (Brutto- und Nettorisiko) nach einheitlichen Maßstäben kalkuliert und beschrieben.

Die Risikolage des Unternehmens und eine eventuelle Bestandsgefährdung werden durch eine Aggregation und Bewertung der Risiken ermittelt. Wechselwirkungen zwischen Risiken werden berücksichtigt.

Prüfung:

Risikoanalyse

Sind für alle gemeldeten Risiken im Risikoinventar Charakter, Eintrittswahrscheinlichkeit sowie Auswirkung (aus der Analyse) erkennbar?

- Interview mit den Verantwortlichen, Sichtung der Dokumentation zur Risikoanalyse.

Werden die erfassten Risiken als Erkenntnis der Analysetätigkeit jeweiligen Risikokategorien zugeordnet, z. B. technologische, operationelle, finanzwirtschaftliche, Branchen- und Marktrisiken, Corporate Governance, politische/rechtliche, strategische Risiken etc? Ist die Zuordnung nachvollziehbar?

- Interview mit den Verantwortlichen, Sichtung des Risikomanagement-Handbuchs, Sichtung des Risikoinventars.
- Gibt es Schnittstellen zu anderen Risikoanalysen , z. B. produktbezogen aus dem Qualitätsmanagement, personalbezogen aus dem Arbeitsschutz- und Gesundheitsmanagement, Umweltmanagement etc., und werden diese Analysen im Risikomanagement berücksichtigt?

Werden bei Anwendung von Meldeschwellen zur lokalen Analyse vergleichbare und einheitliche Methoden verwendet?

- Sind die Meldeschwellen angemessen?
- Stichprobe aus der Übersicht der Risiken, welche die Meldeschwelle nicht überschritten haben. Interview mit dem Analysierenden. Prüfung der sachlichen und rechnerischen Richtigkeit.

Sind die Informationen (Stamm- und Bewegungsdaten), die in die Risikoanalyse einfließen, realistisch?

- Stichprobe aus Risikoinventar und Prüfung durch Interview und Prüfung der sachlichen und rechnerischen Richtigkeit in Bezug auf die angewandten quantitativen Analyseinstrumente sowie möglicherweise Dokumentenprüfung.
- Gegebenenfalls sollte eine Verprobung mit anderen zur Verfügung stehenden Daten erfolgen, z. B. Prüfung Forderungsausfall gegen Schuldenkompass, Sachwerte mit Bilanz oder Gutachten sowie Deckungssummen in Versicherungsverträgen.

Sind die potentiellen Ursachen der Risiken vollständig und plausibel beschrieben?

- Prüfung Risikoinventar.

Sind alle potentiellen und wesentlichen Auswirkungen in voller Bandbreite nachvollziehbar beschrieben?

- Prüfung Risikoinventar.

Ermöglicht es das Risikomanagementsystem, Risiken zu aggregieren und Interdependenzen zu berücksichtigen?

- Werden Korrelationen (Wechselwirkungen) von Risiken berücksichtigt, die zu einer Verstärkung oder Abschwächung der Auswirkungen führen können?
- Prüfung Dokumentation zur Analyse, Interview mit den Verantwortlichen.

Ist definiert, dass die Risikoanalyse nicht nur durch eine einfache Addition von Schadenshöhen erfolgt?

- Interview mit den Verantwortlichen, Sichtung Risikomanagement-Handbuch, Sichtung Risikoberichterstattung und -kommunikation.

Risikobewertung

Sind für alle Risiken Eintrittswahrscheinlichkeit und Auswirkung beschrieben?

- Prüfung des Risikoinventars.

Werden alle Risiken aufgrund einheitlicher Messgrößen für Schadenshöhe und Eintrittswahrscheinlichkeit bewertet?

- Interview mit den Verantwortlichen, Sichtung des Risikomanagement-Handbuchs, Prüfung des Risikoinventars.

Werden je nach Art des Risikos und je nach verfügbaren Informationen Risiken quantitativ oder qualitativ bewertet?

- Prüfung des Risikoinventars, Interview mit den Verantwortlichen.

Gibt es eine einheitliche vorgegebene Bewertungsmethode und wird diese auf qualitative und quantitative Risiken gleich angewendet?

- Werden die richtigen Methoden richtig angewendet? Z. B. Fehler-Möglichkeits-Einflussanalyse (FMEA), Szenario Analyse, Bow-Tie-Analyse, Markov-Analyse, Ishikawa etc.
- Interview mit den Verantwortlichen, Prüfung Arbeitsunterlagen, Protokolle, Sichtung des Risikomanagement-Handbuchs, Prüfung des Risikoinventars.

Werden Risikobewertungen regelmäßig aktualisiert?

- Prüfung des Risikoinventars, Arbeitsunterlagen, Sichtung Risikomanagement-Handbuch, Interview mit den Verantwortlichen.

Werden wesentliche Änderungen der Bewertungen zeitnah aktualisiert?

- Interview mit den Verantwortlichen, Prüfung Eingangsdatum der Meldungen mit dem Aktualisierungsdatum des Risikoinventars.

Basieren quantitative Bewertungen (sofern anwendbar) auf geeigneten Wahrscheinlichkeitsverteilungen, z. B. Binomialverteilung, Dreipunktschätzung, Dreiecksverteilung, Gleichverteilung, kombinierte Verteilungen etc?

- Sind die zugrunde gelegten Daten korrekt?
- Interview mit den Verantwortlichen, Sichtung des Risikomanagement-Handbuchs, Prüfung vorhandener Dokumentation, Prüfung des Risikoinventars.

Wie wird die Risikobewertung plausibilisiert?

- Sachliche und rechnerische Prüfung der Eintrittswahrscheinlichkeit und Auswirkung. Prüfung des Risikoinventars, Sichtung der vorhandenen Dokumentation, Interview mit den Verantwortlichen.

Werden Brutto- und Nettorisiken unterschieden?

Sind Nettorisiken kleiner als Bruttorisiken?

- Plausibilitätsprüfung des Risikoinventars.

Sind die Nettorisiken korrekt aus auf Basis der Maßnahmen (z. B. Versicherung) ermittelt (Wirkungsanalyse)?

- Prüfung des Risikoinventars, Interview mit den Verantwortlichen, Prüfung der vorhandenen Dokumentation.

Sind die Risiken aus verschiedenen Bereichen gleich bewertet worden, so dass eine Vergleichbarkeit besteht?

- Sichtung des Risikomanagement-Handbuchs, Interview mit den Verantwortlichen, Prüfung des Risikoinventars.

Gibt es Kumulrisiken (steigernde Wechselwirkungen von Risiken) und sind diese richtig/nachvollziehbar bewertet?

- Prüfung des Risikoinventars, Sichtung der Dokumentation zur Risikoanalyse, Sichtung des Risikomanagement-Handbuchs, Interview mit den Verantwortlichen.

Gibt es kompensierende Risiken und sind diese richtig bewertet/nachvollziehbar?

- Prüfung des Risikoinventars, Sichtung der Dokumentation zur Risikoanalyse, Sichtung des Risikomanagement-Handbuchs, Interview mit den Verantwortlichen.

Gibt es Sekundärrisiken, die durch Maßnahmen das Risiko noch erhöhen?

- Prüfung des Risikoinventars, Sichtung der Dokumentation zur Risikoanalyse, Sichtung des Risikomanagement-Handbuchs, Interview mit den Verantwortlichen.

(Wie) Wird ein Gesamtrisikoumfang des Unternehmens ermittelt?

- Werden Risikoerwartungswerte einfach addiert oder eine Risikoaggregation durchgeführt (z. B. mit einer Monte Carlo Simulation)?
- Interview mit den Verantwortlichen, Prüfung der Risikoberichte und des Risikoinventars, Sichtung des Risikomanagement-Handbuchs, Sichtung einer entsprechenden Dokumentation.

6.5 Risikosteuerung und –überwachung

Sollzustand:

Für alle wesentlichen Risiken sind Maßnahmen implementiert, die in ihrer Summe geeignet sind, mit angemessener Sicherheit den Weiterbestand der Organisation zu sichern.

Hergeleitete Risikobewältigungs-Maßnahmen steuern die identifizierten und analysierten Risiken im Einklang mit der Risikostrategie.

Die gewählten Maßnahmen sind angemessen und wirksam, um die Risiken zu behandeln.

Die Risikoüberwachung erfolgt sowohl beim operativen Management (Risikoverantwortliche) als auch bei zentralen Überwachungsfunktionen (Risikomanagement, Risikocontrol-

ling etc.). Ergänzt wird die Überwachung durch unabhängige und objektive Prüfungen der Internen Revision.

Prüfung:

Risikosteuerung

Wurden für alle wesentlichen Risiken Bewältigungsmaßnahmen definiert?

- Prüfung der wesentlichen Risiken und der entsprechenden Maßnahmen (ggf. Stichproben). Interview mit den Verantwortlichen.

Wurden bei der Festlegung der Bewältigungsmaßnahmen Kosten-Nutzen-Überlegungen mit einbezogen?

- Prüfung des Risikoregisters, Sichtung der Details zu den jeweiligen Bewältigungsmaßnahmen, Interview mit den Verantwortlichen hinsichtlich Kosten-Nutzen-Analysen.

Wurde bei der Einführung technischer Maßnahmen für ausreichende Ausfallsicherheit und Notfallplanung gesorgt?

- Interview mit den Verantwortlichen, Sichtung von Nachweisen (Protokolle etc.).

Wurde bei organisatorischen Maßnahmen auf die Möglichkeit der Umgehung der Maßnahmen geachtet und ausreichendes Monitoring eingerichtet?

- Interview mit den Verantwortlichen, Einsichtnahme in Nachweise.

Wurden bei personellen Maßnahmen alle betroffenen Mitarbeiter ausreichend geschult und mit den nötigen Ressourcen versehen?

- Interview mit den Verantwortlichen, Prüfung Risikomanagement-Handbuch etc. auf entsprechend einzuhaltende Vorgaben, Einsichtnahme in Schulungsnachweise.

Gibt es ausreichende Vertretungs- und Nachfolgeregelungen, die den Fortbestand der Risikobewältigungsmaßnahmen auch bei Personalausfall bzw. -änderung gewährleisten?

- Interview mit den Verantwortlichen, Prüfung Risikomanagement-Handbuch etc. auf entsprechend einzuhaltende Vorgaben, Einsichtnahme in Vertretungsregelungen, Walk-Through mit stichprobenartig ausgewählten Maßnahmenverantwortlichen.

Wurde bei der Auswahl der Maßnahmen die Wechselwirkung mit anderen Risiken berücksichtigt?

- Interview mit den Verantwortlichen, Einsichtnahme in die entsprechende Dokumentation. Abgleich der Maßnahmen von Risiken, bei denen im Rahmen der Analyse Wechselwirkungen festgestellt wurden.

Ermöglichen die gewählten Risikobewältigungsmaßnahmen in ausreichendem Maß eine wirtschaftliche Weiterführung der Geschäftsprozesse? Werden Chancen in ausreichendem Maß berücksichtigt?

- Interview mit den Verantwortlichen, Einsichtnahme Dokumentationen, Walk-Through.

Wurden auch Maßnahmen für die Bewältigung von Risiken getroffen, deren Eintritt zwar sehr unwahrscheinlich, deren Auswirkung aber bestandsgefährdend für die Organisation ist?

- Interview mit den Verantwortlichen, Auswahl der entsprechenden Risiken, Plausibilisierung der Risikostrategien und Maßnahmen.

Wurde in jenen Fällen, in denen Risiken bewusst getragen werden, das Vorhandensein der dafür notwendigen Kapitaldeckung ermittelt?

- Interview mit den Verantwortlichen, Einsichtnahme in die Dokumentation (z. B. Analyse).

Risikoüberwachung

Beinhaltet das Risikomanagement ein Frühwarnsystem?

- Gewährleistet das Frühwarnsystem, dass notwendige Maßnahmen zur Anpassung der Risikobewältigungsmaßnahmen rechtzeitig ergriffen werden können?
- Wurden Indikatoren und entsprechende Grenzwerte definiert? Sind diese angemessen?
- Werden die Grenzwerte überwacht? Von wem? Wie oft?
- Sind Maßnahmen definiert für den Fall, dass Grenzwerte überschritten werden?
- Ermöglichen die Indikatoren, die Veränderungen eines Risikos im Zeitablauf zu messen und zu beurteilen?
- Sichtung des Risikomanagement-Handbuchs, Interview mit den Verantwortlichen, stichprobenartige Auswahl an Risiken mit möglichem Frühwarnsystem und Walk-Through, Prüfung des Monitorings der Indikatoren, Plausibilisierung der Grenzwerte, Prüfung vorliegender Maßnahmenpläne für die Überschreitung von Grenzwerten.

Sind die gewählten Maßnahmen im Einklang mit der Risikostrategie des Unternehmens?

- Interview mit den Verantwortlichen, Abgleich stichprobenartig gewählter Maßnahmen mit der Risikostrategie des Unternehmens.

Haben die gewählten Maßnahmen einen Einfluss auf die Eintrittswahrscheinlichkeit und/oder der Auswirkung der Risiken?

- Interview mit den Verantwortlichen, Sichtung des Risikoinventars, Prüfung und Plausibilisierung der Maßnahmeneffekte.

6.6 Risikoberichterstattung und -kommunikation

Sollzustand:

Entscheidungsträger und Aufsichtsorgane sind zeitnah, vollständig und korrekt über die Risikolage des Unternehmens informiert.

Die Unternehmensleitung und Aufsichtsorgane werden regelmäßig über den Aufbau sowie über den Stand der Umsetzung des Risikomanagementsystems, das Ergebnis der Risikoinventur und der Überwachungssysteme in Kenntnis gesetzt.

Prüfung:

Sind die Vorgaben für eine interne Risikoberichterstattung und -kommunikation vorhanden und angemessen?

- Sichtung des Risikomanagement-Handbuchs, Interview mit den Verantwortlichen.

Ist definiert,

- was zu berichten ist (Risiken, Bewertungen, Maßnahmen, Indikatoren, Risikoverantwortlicher, Maßnahmenverantwortlicher, Maßnahmenstatus, Ursachen, Auswirkungen, Wechselwirkungen, Risikotrend/-entwicklung, Risikostrategie (Risiko vermeiden, vermindern, transferieren, akzeptieren), Risikoaggregation etc.),
- welche Risikokategorien genannt werden,
- welche Wesentlichkeitsgrenzen beachtet werden müssen,
- welcher Berichtszyklus anwendbar ist (regelmäßig, ad hoc),
- welches Berichtsmedium und welches Format angewendet werden soll,
- ob eine Brutto- oder Nettoberichterstattung erfolgt,
- wer Berichtersteller und Empfänger sind?
- Sichtung des Risikomanagement-Handbuchs, Interview mit den Verantwortlichen, Abgleich der Vorgaben mit Nachweisen der tatsächlichen Berichterstattung und Kommunikation.

Sind gesetzliche Meldeverpflichtungen vorhanden? Ist ein entsprechend geeigneter Prozess mit vorgelagerten Schwellenwerten und Warnhinweisen vorhanden?

- Sichtung des Risikomanagement-Handbuchs, Interview mit den Verantwortlichen, Abgleich mit Nachweisen der tatsächlichen Berichterstattung und Kommunikation.

Ist die Berichterstattung verständlich, vollständig, zeitnah, entscheidungsrelevant und adressatengerecht (verständlich, transparent)?

- Einsichtnahme in die Berichterstattung, Abgleich mit vorhandenen Vorgaben.

Ist der Prozess der Ad-hoc-Berichterstattung definiert?

- Ist dieser angemessen und wird er eingehalten?
- Sichtung des Risikomanagement-Handbuchs, Interview mit den Verantwortlichen, Abgleich der Vorgaben mit Nachweisen der tatsächlichen Berichterstattung und Kommunikation.

7 Zusammenarbeit zwischen Interner Revision und Abschlussprüfer im Rahmen des Risikomanagementsystems

7.1 Prüfungsstandards

Die Zusammenarbeit zwischen Interner Revision und Wirtschaftsprüfer wird generell im DIIR Revisionsstandard Nr. 1 „Zusammenarbeit von Interner Revision und Abschlussprüfer“ geregelt.

Zwar dürfen die Ergebnisse der Internen Revision die eigenen Prüfungshandlungen des Abschlussprüfers nicht ersetzen, eine Kooperation der beiden Überwachungsorgane mit einem regelmäßigen Informationsaustausch wird jedoch ausdrücklich nahegelegt.

Für Kapitalgesellschaften ergeben sich aus Abschnitt 3.5 Tz. 16 des IDW PS 340 „Die Prüfung des Risikofrüherkennungssystems nach § 317 Abs. 4 HGB“ Anforderungen an die Interne Revision. Das Risikomanagementsystem eines Unternehmens wird ausdrücklich als Prüfungsgegenstand der Internen Revision genannt. Diese Prüfungstätigkeit der Internen Revision ist auch Teil der Gesamtbeurteilung des Abschlussprüfers (Abschn. 4.3.2, Tz. 29).

Gemäß IDW Prüfungsstandard soll die Interne Revision die Wirksamkeit des Risikomanagementsystems im Rahmen einer Ordnungsmäßigkeitsprüfung untersuchen. Die Prüfung kann u. a. die folgenden Aspekte beinhalten:

- Vollständigkeit der Erfassung aller Risikofelder,
- Angemessenheit der eingerichteten Maßnahmen zur Risikoerfassung und Risikokommunikation,
- Kontinuität der Anwendung der Maßnahmen und Einhaltung der integrierten Kontrollen.

Gemäß IDW PS 321 „Interne Revision und Abschlussprüfung“ stützt sich der Abschlussprüfer regelmäßig auf Feststellungen der Internen Revision. Auch bei der Verwertung der Arbeiten der Internen Revision behält der Abschlussprüfer weiterhin die alleinige und unteilbare Verantwortung für das Prüfungsurteil.

Eine Eingliederung von Personal der Internen Revision in das Prüfungsteam des Abschlussprüfers ist zudem nicht zulässig.

Bei öffentlich-rechtlichen Unternehmen, die gemäß IDW PS 720 „Berichterstattung über die Erweiterung der Abschlussprüfung nach § 53 HGrG“ geprüft werden, erstreckt sich der Prüfungsumfang des o. a. Standards sowohl auf das Vorhandensein – und in gewissem Umfang auf die Angemessenheit – des Risikomanagements als auch auf die Interne Revision. Insofern bietet sich hier ein Dialog mit dem Abschlussprüfer auf Basis der zum IDW PS 720 gehörenden Fragebögen (jeweils zu „Risikofrüherkennungssystem“ und „Interne Revision“) an.

Durch eine angemessen gestaltete Kooperation können u. a. die folgenden Vorteile entstehen:

- Vermeiden von Redundanzen und Doppelarbeiten,
- geringere Kosten,
- höhere Prüffeldabdeckung,
- Qualitätssteigerungen,
- reduziertes Überwachungsrisiko,
- Feedback der Abschlussprüfer als Möglichkeit zur Verbesserung der internen Revisionsfunktion

7.2 Mögliche Zusammenarbeit in der Praxis

Phase Prüfungsplanung:

- Austauschen von (vorläufigen) Risikoeinschätzungen
- Vermeiden von Doppelarbeiten
- Abstimmen von Prüfungsschwerpunkten

Phase Prüfungsdurchführung:

- Abstimmen von Checklisten, Dokumentationsformen etc.
- Zeitliches Koordinieren der Prüfungen

Phase Berichterstellung:

- Austauschen von Ergebnissen und Berichten
- Nutzen der Kenntnisse der Internen Revision zur Beurteilung des Lageberichtes

Phase Follow-up:

- Übernehmen der Ergebnisse der Jahresabschlussprüfung in die Follow-up Datenbank der Internen Revision
- Austauschen von Anhaltspunkten für Planung von Folgeprüfungen

8 Anhang

8.1 Musterliste zur Vollständigkeitsprüfung

Externe Risiken und mögliche Prüfungshandlungen	
Wettbewerbsrechtliche Risiken	
Verstoß gegen Wettbewerbsrecht, z. B. Preisabsprachen, Kartelle, unlauterer Wettbewerb, Auflagen	Analyse Risikoinventar, Interview Rechtsabteilung/Vertrieb, Markterkundung
Marktrisiko (Mengen-/Preisrisiko)	
Preisrückgang/Verfall (z. B. durch Wettbewerb), Erreichen Grenzpreis, Mengenrückgang, Überkapazität, Dumping, Marktbeschränkungen	Analyse Risikoinventar, Preisanalyse, Interview Vertrieb/Controlling, Trendanalyse, Fachzeitschriften, Prognosen, vorhandene Gutachten, Markterkundung
Branchen- und Produktfehlentwicklung	
nicht Akzeptanz bestimmter Produkte (Nahrungszusätze, Pelze, Zigaretten etc.)	Analyse Risikoinventar, Prüfung Social Media, vorhandene Analysen Vertrieb, Interview
Steuerrisiko	
umsatzsteuerfreie Lieferungen, Steuererhöhungen/Einführung neue Steuern, Bewertungsunterschiede, Veränderung Zölle, Betriebsprüfungen, Strafzinsen	Analyse Risikoinventar, Dokumenten- und Prozessprüfung (z. B. Verbringungsnachweise), Interview verantwortliches Management (z. B. Steuerabteilung/Finanzbereich), Ergebnisse der letzten Betriebsprüfung
Politische und rechtliche Entwicklung	
ungünstige Verbote- und Gebote, Veränderung Subventionen, Änderungen Gesellschaftsrecht (z. B. Rechtsformen), Enteignung	Analyse Risikoinventar, Interview verantwortliches Management (z. B. Lobbying), Analyse, Presse und Fachabteilungen/Verbände, Gefährdungskarten
Umweltkatastrophen/Krieg	
Krieg, innere Unruhe, Terrorismus, Erdbeben, Hochwasser, Vulkanausbrüche, Kometeneinschlag, Blitzschlag, Feuer, Pandemie, Occupy	Analyse Risikoinventar, Interview verantwortliches Management (Vorstand/Leitung Facility Management), Maßnahmenliste, Prüfung Versicherungsgutachten, Gefährdungskarten

Strategische Risiken und mögliche Prüfungshandlungen

Verlust aus Beteiligungen	
(Teilwert-)Abschreibungen, Verlustübernahmeverträge, Liquiditätsengpässe	Analyse Risikoinventar, Prüfung Bilanz, Investitionsrechnung, Due Diligence Bericht, Interview, Gutachten zur Werthaltigkeit
Produkt	
falsches Produktportfolio (nicht zeitgemäß etc.), zu viele Produkte in derselben Phase des Produktlebenszyklus, Fehlentscheidungen in der Produktbeschaffenheit, fehlendes Produkt	Analyse Risikoinventar, Marktanalyse, Interview verantwortliches Management, Abhängigkeit Vertrieb/Produktion/Marketing/Produktmanagement (z. B. auf Basis Meeting-Protokoll)
Investitionen	
Fehlinvestitionen, fehlende Amortisation, zu hohe Investition (z. B. Liquidität, Beherrschbarkeit), nicht Eintreten von Annahmen, fehlende Investitionen	Analyse Risikoinventar, Analyse der Investitionsübersicht und Investitionsrechnung (z. B. Szenarioanalyse), Prüfung der Risiken aus abgelehnten Investitionsanträgen, Prüfung Genehmigungen von Investitionen
Standort	
logistisch falscher Standort, Standort mit wenig Publikumsverkehr, fallende Grundstückspreise	Analyse Risikoinventar, Prüfung Standortanalyse, Grundstückspreisentwicklung, Interview
Informationsmanagement	
Beschaffung, falsche Informationsbeschaffung/-basis, Verarbeitung, falsche Software- Ausrüstungsentscheidung, fehlerhafter Aufbau Architektur	Analyse Risikoinventar, Interview/Protokolle verantwortliches Management, Protokolle verantwortliches Management, Investitionsentscheidungen, Prüfung Übersicht Software und Architektur, IT Trendanalyse
Länderrisiken	
Kultur falsch eingeschätzt, Transportkosten, neue Gesetze, Sprachbarrieren, Ethik	Analyse Risikoinventar, Interview/Protokolle verantwortliches Management, Auswärtiges Amt
Einkauf	
Lieferantenstrategie, Hedging, Vergaberisiken, Make or Buy	Analyse Risikoinventar, Interviews mit Risikoverantwortlichen, Prüfung Make-or-Buy-Berechnungsgrundlagen

Operative Risiken und mögliche Prüfungshandlungen

Produkt	
Produkt trifft nicht den Kundenbedarf/die Kundenanforderungen, Wettbewerbsprodukte bieten besseres Preis-Leistungsverhältnis oder Zusatznutzen, Sicherheitsrisiken, verbunden mit Rückruf und/oder Imageverlust	Analyse Risikoinventar, Interviews mit Verantwortlichen und mit Vertrieb
Fertigung	
Nacharbeitskosten, Qualitätsmängel, fehlende Produktivität, veralteter Maschinenpark, hoher Instanthaltungsaufwand, Stillstandkosten	Analyse Altersstruktur Anlagevermögen, Instandhaltungskosten, Analyse Reklamationen, Interviews mit Fertigungsleitung und mit Qualitätsmanagement
Kapazität	
Wachstums- und Ertragschancen können nicht genutzt werden, alternativ: zu hohe Fixkosten bei fehlender Auslastung	Analyse Risikoinventar, Analyse Auslastungsgrad im Zeitverlauf
Lieferanten	
Lieferengpässe durch fehlende Kapazität (vor allem bei single sourcing), Abhängigkeit von Lieferanten	Analyse der Lieferantenstruktur und Lieferantenbewertung, Auflistung Alternativlieferanten nach Produktgruppen, Interviews mit Verantwortlichen
Lagerhaltung	
Elementarschäden, Feuer, Wasser; Diebstahl, Beschädigung	Analyse Risikoinventar, Prüfung Schutzmaßnahmen, Analyse Sachversicherung
Logistik	
Engpässe durch zu lange Logistikkette, steigende Transportkosten	Analyse Risikoinventar, Interviews mit Verantwortlichen
Umweltmanagement	
unklare Regelungen von Verantwortungen, Aufgaben und Kompetenzen (auch für Kontrollen), fehlende Gesetzeskenntnisse und fehlende Kontrolle auf deren Einhaltung; Emissionsschäden durch Lackieranlagen, Imageschäden, z. B. durch negative CO2-Bilanz, unzureichende technische Schutzmaßnahmen	Analyse Risikoinventar, Prüfung Schutzmaßnahmen, Analyse Sachversicherung, Interviews
Warenzeichen/Patente	
Diebstahl, Missbrauch	Analyse Risikoinventar, Interviews

Öffentlich-rechtliche Genehmigungen	
fehlende Ausfuhrgenehmigung (BAFA), unerlaubter TK-Betrieb (Bundesnetzagentur), unterlassene Meldung beim LDSB (Personendaten)	Analyse Risikoinventar, Vorlage und Prüfung von regulatorischen Dokumenten, Abgleich Compliance-Aufstellung
Gewährleistung/Haftungsrisiken	
Produkthaftung/Produktsicherheit, Mängel in der Dienstleistungserbringung, versteckte Qualitätsmängel, Folgeschäden beim Abnehmer	Analyse Risikoinventar, Vorlage FMEA (o. Ä.), Vorlage Versicherungspolicen, Interview Rechtsabteilung/ggf. Produktion/Entwicklung
Personengefährdung/Arbeitsschutz	
unzureichende Schutzkleidung, Verstoß gegen Gefahrstoffverordnung, ungesicherte Maschinen, unqualifizierte bedienende Personen, unzureichende Organisation des Arbeits- und Gesundheitsschutzes, mangelnde Ein- bzw. Unterweisung, fehlende arbeitsmedizinische Betreuung.	Analyse Risikoinventar, Interview Arbeitsschutzbeauftragter, Vorlage Arbeitsschutzkonzept, ggf. Zertifikate (OHSAS18001), Ergebnisse von Begehungen durch Berufsgenossenschaften, Dokumentation von extern eingesetzten Arbeitsschutz-Dienstleistern
Steuerungssysteme	
falsche Berechnungsgrundlage Produktionsplanung, ungeeignete KPI, fehlerhafte Managementinformation, multivariable Aussagen	Analyse Risikoinventar, Vorlage FMEA, Markov-Analyse, Ishikawa-Diagramme etc.
Kontrollsysteme	
keine Funktionstrennung (SoD), fehlendes 4-Augen-Prinzip, keine Eingabekontrollen bei IT- und Webapplikationen etc.	Analyse Risikoinventar, Szenarioanalyse, Revisionsunterlagen
Investitionen/Ersatzbeschaffungen	
fehlende/unzureichende Investitionen, Betriebsunterbrechungen, überhöhte Wartungskosten, überhöhte Kosten für kurzfristige Ersatzbeschaffungen, Qualitätsmängel	Analyse Risikoinventar, Interview

Personalrisiken und mögliche Prüfungshandlungen

Management Nachfolgeregelung	
unzureichende Nachfolgeregelung, Ausfall Know-how-Träger (Wissens- und Leistungsträger), Betriebsunterbrechungen	Analyse Risikoinventar, Vorlage Altersstruktur, strategische Personalplanung, Interview Personalleitung

Qualifikation/Fachkräftemangel	
unzureichende Qualifikation des Personals, Wettbewerbsnachteile, Qualitätsprobleme, Abweichungen von Vorgaben, Betriebsunterbrechungen, verhindertes Wachstum	Analyse Risikoinventar, Vorlage Qualifikationsanforderungen, Interview Personalleitung/-entwicklung, Trends Bewerbungseingänge, Schulungs- und Weiterbildungskonzepte
Integrität und dolose Handlungen	
negatives Image, negative Berichterstattung, verunsicherte Stakeholder, Rechtsprozesse und -kosten, Haftungsrisiken, Beeinträchtigung einer Compliance-Kultur, Mitarbeiterunzufriedenheit, negatives Betriebsklima, erschwertes Recruiting	Analyse Risikoinventar, eigene Revisionsunterlagen, Ethik-Richtlinie, Vorbeugemaßnahmen/Awareness, Interview Rechtsabteilung, eingegangene Meldungen Compliance-Hotline
Fluktuation	
Betriebsunterbrechungen, verhindertes Wachstum, Kosten für Einarbeitung, Ausbildung und Qualifizierung, Weggang Know-how(-Träger), Recruiting-Kosten	Analyse Risikoinventar, Ein- und Austritte 3 Jahre, Interview mit Personalleitung, Benchmarking mit vergleichbaren Unternehmen
Tarifgestaltung	
unflexible Funktionsbeschreibungen, fehlende Motivation durch starres Einstufungskonzept, zu formaler/zeitaufwändiger Umgang mit Betriebsrat	Analyse Risikoinventar, Vorlage Einstufungskonzept, Tarifvertrag, Vereinbarungen mit Betriebs-/Personalrat
Demografische Entwicklung	
nicht adäquate Entwicklung von Führungskräften und Mitarbeitern, hohes Durchschnittsalter bei Verantwortlichen in Schlüsselpositionen und Mitarbeitern, fehlende frühzeitige Nachfolgeregelung	Analyse Risikoinventar, Vorlage Altersstruktur, strategische Personalplanung, Einzelmaßnahmen, Gesundheitsmanagement, Interview Personalleitung
Vertretungsregelung	
fehlende oder unvollständige Festlegung bzw. Dokumentation, mangelnde Kompetenz der Stellvertreter	Analyse Risikoinventar, Vorlage Vollmachtenregelung, Organigramm, Vollmachtenvergabe (Stichprobe)
Corporate Social Responsibility	
fehlende Richtlinie zu CSR und/oder Ethik, Ungleichbehandlung von Mitarbeitern, mangelnde Gesetzeskenntnisse in Ländern mit Niederlassungen, keine Kontrolle auf Einhaltung in den Ländern	Analyse Risikoinventar, Interview mit betroffenen Führungskräften (Personal, Produktion, Presse-/Öffentlichkeitsarbeit)

Datenverarbeitungsrisiken und mögliche Prüfungshandlungen

Integrität	
unzureichende funktionsweise wichtiger Systeme (z. B. Produktion, ERP, Sicherheit), Datenbank ist nicht mehr konsistent, (teilweise) fehlende Indices, fehlende Datensätze, Hackerangriffe/Schadsoftware	Analyse Risikoinventar, Szenarioanalyse, Systemprüfung: Zugriffsrechte, Schutz nach außen und innen, Transportwege, Anwendungsprüfung: EVA (Eingabe, Verarbeitung, Ausgabe), vorhandene „Application controls“
Vertraulichkeit	
fehlende/unzureichende Zugangskontrolle zu vertraulichen Daten, Datendiebstahl von außen/von innen, Hackerangriffe/Schadsoftware	Analyse Risikoinventar, Szenarioanalyse, Systemprüfung: Zugriffsrechte, Schutz nach außen und innen, Transportwege, Vertraulichkeitsvereinbarung, Awareness, Rollen- und Berechtigungssystem
Verfügbarkeit	
Ausfall/Datenverlust wichtiger Systeme (z. B. Produktion, ERP, Sicherheit), fehlende/unzureichende Datensicherung, unzureichende Desaster Recovery Prozesse (DRP)	Analyse Risikoinventar, Szenarioanalyse, Datensicherungskonzept, Auslagerung, BCM

Finanzwirtschaftliche Risiken und mögliche Prüfungshandlungen

Liquidität	
unzureichende Mittel für geplante/ungeplante Zahlungsausgänge, Kreditkündigung, Zahlungsausfälle	Analyse Risikoinventar, Prüfung der Risikobewältigungsmaßnahmen (Existenz, Wirksamkeit, Effizienz etc.), Interviews, Analyse liquider Mittel, Abgleich gegen geplante Zahlungsverpflichtungen, Prüfung Kreditlinien
Wechselkursrisiken	
z. B. Geldanlage oder Aufnahme in Fremdwährung, Bewertung Beteiligungen Fremdwährung, Einkaufpreise in Fremdwährung, Wettbewerbsfähigkeit in FW-Märkten, Bewertung Kurssicherungsgeschäfte (Derivate etc.)	Analyse Risikoinventar, Szenarioanalyse, Prüfung der Risikobewältigungsmaßnahmen (Existenz, Wirksamkeit, Effizienz etc.), Interviews, Plausibilisierung Hedging-Strategien (ggf. Einbeziehen von Experten)
Zinsänderungsrisiken	
z. B. Verminderung Anlage- oder Erhöhung Kreditaufnahmezins, Bewertung Zinsderivate	Analyse Risikoinventar, Szenarioanalyse, Prüfung der Risikobewältigungsmaßnahmen (Existenz, Wirksamkeit, Effizienz etc.), Interviews

Wertpapierkursrisiken	
Entwicklung des Aktienmarkts, Bewertungsschwankungen, Branchenrisiken	Analyse Risikoinventar, Szenarioanalyse, Prüfung der Risikobewältigungsmaßnahmen (Existenz, Wirksamkeit, Effizienz etc.), Interviews, Analyse Kurssicherungsstrategien (Hedging)
Adressenausfallrisiken	
Insolvenz von Debitoren, lange Überfälligkeiten, Länderrisiken	Analyse Risikoinventar, Prüfung der Risikobewältigungsmaßnahmen (Existenz, Wirksamkeit, Effizienz etc.), Interviews (z. B. mit dem Forderungsmanagement), Analyse Altersstruktur Forderungen, Trendanalyse Forderungsausfälle, Benchmarking mit vergleichbaren Unternehmen, Prüfung Kontrollen zum Liquiditätscheck und Monitoring von Debitoren

Compliance Risiken und mögliche Prüfungshandlungen

Corporate Governance	
Vertrauensverluste bei Stakeholdern (Eigentümer, internationale und nationale Anleger, Öffentlichkeit, Lieferanten, Gläubiger, Mitarbeiter etc.), finanzielle Verluste (bis hin zur Insolvenz), Imageverlust, Bußgelder, Strafzahlungen, Rechtsprozesse, persönliche Haftung	Analyse Risikoinventar, Analyse eines internen Corporate Governance Frameworks (z. B. Dokumentation, Code of Conduct, Definition von Verantwortlichkeiten, Ethik Code, Gruppen- und lokale Richtlinien (HR, Recht, IT …), Benchmarking mit Frameworks vergleichbarer Unternehmen, organisatorische Beurteilung, ob die Organisation zum Corporate Governance Framework passt (Angemessenheit), Interviews (z. B. mit Unternehmensleitung, Revision, Compliance, Recht, Risikomanagement etc.), Sichtung (Presse-)Berichterstattung, Sichtung wesentlicher Vorfälle und Ursachenanalyse etc.
Ethik & Compliance	
unzureichender "tone from the top", Imageverlust, Bußgelder und Haftstrafen, Sanktionen aufgrund Nicht-Einhaltung von Vorschriften, Gesetzen oder Normen und vertraglichen Vereinbarungen, Ausschluss vom Wettbewerb (z. B. vom Vergabeverfahren, „Black List“), finanzielle Verluste (bis hin zur Insolvenz), Mitarbeiterunzufriedenheit/belastetes Betriebsklima	Analyse Risikoinventar, Analyse eines internen Corporate Governance Frameworks, organisatorische Beurteilung, ob die Organisation zum Corporate Governance Framework passt (Angemessenheit), Interviews (z. B. mit Unternehmensleitung, Revision, Compliance, CSR, Recht, Risikomanagement etc.), Sichtung (Presse-) Berichterstattung, Sichtung wesentlicher Vorfälle und Ursachenanalyse etc.

Verstoß gegen Wettbewerbsrecht	
Preisabsprachen/Kartelle/unlauterer Wettbewerb, Schadensersatzansprüche, Straftatbestand (Geld-/Freiheitsstrafe), Kündigung/Verlust von Aufträgen, finanzielle Verluste (bis hin zur Insolvenz)	Analyse Risikoinventar, Analyse eines internen Corporate Governance Frameworks, Interviews (z. B. mit Unternehmensleitung, Revision, Compliance, CSR, Recht, Risikomanagement, Vertrieb, Einkauf etc.), Sichtung (Presse-)Berichterstattung, Sichtung wesentlicher Vorfälle und Ursachenanalyse etc., Prüfung einer Auflistung von Kooperationen mit anderen Unternehmen (mit potentiell wettbewerbsrechtlicher Relevanz)

8.2 Fragenkatalog

Nr.	Frage	Art der Prüfung		Interview-partner	Dokumentation der Prüfungsergebnisse		
		Sichtprüfung, Systemprüfung, Interview, ...	ggf. Stich-probenan-zahl	Name, Funk-tion	ggf. ja/nein		Verweise auf Anlagen, Stichproben oder detaillierte Beschreibung des Sachverhalts
1.0	**Risikomanagement-Organisation**						
1.1	Aus welchem Grund wurde ein Risikomanagement eingeführt? (Rechtl. Verpflichtung? Freiwillig?)						
1.2	Ist das Risikomanagement auf geeignete Art und Weise in die Gesamtor-ganisation integriert?						
1.3	Wer/wie viele Mitarbeiter sind für das RM verantwortlich?						
1.4	Gibt es eine schriftliche Grundlage für die Verfahrensweise im Rahmen des Risikomanagements?						
1.5	Wurden die Grundlagen des Risikomanagements (Grund für die Einrich-tung, Verantwortlichkeiten usw.) an alle Mitarbeiter des Unternehmens						

	kommuniziert?						
1.7	Wurden die Mitarbeiter in geeigneter Form (z.B. Workshops, Interne Mitteilungen, Schulungen) über die Grundlagen des Risikomanagements informiert?						
1.8	Erfolgt an die Mitarbeiter regelmäßig eine Erinnerung an die Grundlagen und Ziele des Risikomanagement?						
2.0	**Risikostrategie**						
2.1	Wurde eine Risikostrategie und -politik definiert? Ist diese schriftlich festgehalten?						
2.2	Werden für die Bewältigung von verschiedenen Risiken gemeinsame Strategien definiert?						
2.3	Werden bei der Risiko-Bewältigung gleichartige Risiken zusammengefasst?						
3.0	**Risikoidentifikation und -erfassung**						
3.1	Werden die richtigen Methoden richtig angewendet? (bspw. FMEA, Szenario-Analyse, Brainstorming, Workshops, Morphologische Matrix, Delphi-Methode, strukturierte Interviews, Gesprächsleitfäden, SWOT-Analyse, Markt- und Wettbewerbsanalyse etc.)						
3.2	Wenn Workshops stattfinden, wer sind die Teilnehmer? (Nehmen z.B. nur das nationale Management bzw. Fachleute teil oder wird nur national beurteilt?)						
3.3	Wenn Frage- oder Erfassungsbögen verwendet werden, wie ist der Rück-						

	lauf? Gibt es eine Ausgrenzung einzelner Bereiche?						
3.4	Erfolgt die Identifikation der auf das Unternehmen einwirkenden Risiken anhand der Wertschöpfungskette oder entlang der Funktionsbereiche?						
3.5	Wurden die in die Zukunft reichenden strategischen Entscheidungen mit den dazugehörigen Risiken betrachtet?						
3.6	Erfolgt eine sinnvoll gestaltete Einteilung der Risiken in Risikofelder?						
3.7	Ist sichergestellt, dass alle Unternehmensbereiche einschl. des Vorstandes bzw. der Geschäftsführung in das Risikomanagement einbezogen sind?						
3.8	Sind alle wesentlichen Betriebsstellen, Geschäftsbereiche, Geschäftsfelder, Prozesse etc. in das RM eingebunden?						
3.9	Erfolgt die Risikodefinition nach dem Top-Down-Prinzip? Gibt es im Unternehmen ein einheitliches Verständnis von "Risiko"?						
3.10	Erfolgt die Risikoidentifikation nach dem Bottom-Up-Prinzip?						
3.11	Wer ist für die Risikoidentifikation und Erfassung verantwortlich? Gibt es eine Dokumentation, die Verantwortlichkeiten fest zuteilt?						
3.12	Erfolgt die Erfassung zentral oder dezentral? Gibt es für eine dezentrale Erfassung beratende Ansprechpartner?						
3.13	Erfolgt eine Fokussierung des Risikomanagement (z.B. Schadenshöhe und Eintrittswahrscheinlichkeit)?						
3.14	Ist die Identifikation der wesentlichen Risiken sichergestellt?						
3.15	Lassen sich wesentliche Risiken aus den Aufgaben und Zielen des Unter-						

	nehmens ableiten? Sind diese im Risikoinventar berücksichtigt?						
3.16	Werden durch die Interne Revision oder den Abschlussprüfer festgestellte Risiken mit in das Risikoinventar aufgenommen?						
3.17	Wie wird sichergestellt, dass Risikomeldungen vergleichbar sind? Gibt es einen formalen Prozess, Formulare, Leitfäden etc.?						
3.18	Sind alle gemeldeten Risiken im Risikoinventar aufgeführt?						
3.19	Wie wird eine Vollständigkeit des Risikoinventars sichergestellt? Werden bspw. mögliche Risiken/Musterlisten mit dem Risikoinventar abgeglichen? Kann das Fehlen bestimmter Risiken begründet werden?						
3.20	Ist sichergestellt, dass Veränderungen in der Risikolandschaft des Unternehmens auch im Risikomanagement berücksichtigt werden?						
3.21	Sind das politische und das rechtliche Umfeld bei der Erstellung des Risikoinventars berücksichtigt?						
3.22	Wird nach der Ermittlung der einzelnen Risiken ein Risikoinventar aufgestellt?						
3.23	Werden Doppelnennungen von Risiken im Risikoinventar vermieden?						
3.24	Wird eine Risikoinventur mindestens einmal im Geschäftsjahr durchgeführt?						
3.25	Wie aktuell ist das Risikoinventar?						
3.26	Ist sichergestellt, dass unterjährig neu auftretende Risiken zeitnah identifiziert und gemeldet werden?						

3.27	Wird übe neue Risiken nachgedacht? Gibt es über Jahre gleichbleibende Risiken, obwohl sich z.B. das Geschäftsmodell/die Unternehmensstrategie oder das Unternehmensumfeld (rechtlich, gesetzlich, politisch, technisch) verändert hat?						
3.28	Erfolgt zur Beurteilung der Risikosituation eine quantitative Aggregation aller Risiken nach einem anerkannten Verfahren (z.B. Value at Risk, Szenario-Berechnung, Monte-Carlo-Simulation)?						
3.29	Werden die Ergebnisse aus der Risikoaggregation in der Unternehmensplanung berücksichtigt?						
3.30	Wird die Risikosituation zusätzlich durch eine qualitative Analyse der Risiken bewertet?						
4.0	**Risikoanalyse und -bewertung**						
4.1	Sind für alle gemeldeten Risiken im Risikoinventar Charakter, Eintrittswahrscheinlichkeit sowie Auswirkung aus der Analyse erkennbar?						
4.2	Werden alle Risiken aufgrund einheitlicher Messgrößen für Schadenshöhe und Eintrittswahrscheinlichkeit bewertet?						
4.3	Erfolgt die Einstufung der Risiken im Risikoportfolio nach den gleichen Kriterien?						
4.4	Werden die erfassten Risiken als Erkenntnis der Analysetätigkeit jeweiligen Risikokategorien zugeordnet? Z.B. technologische, operationelle, finanzwirtschaftliche, Branchen- und Marktrisiken, Corporate Governance, politische/rechtliche, strategische etc.? Ist die Zuordnung nachvollziehbar?						

4.5	Werden alle Risiken in ein Risikoportfolio übertragen und aufgrund von Klassifizierungen bewertet?						
4.6	Werden je nach Art des Risikos und je nach verfügbaren Informationen quantitativ oder qualitativ bewertet?						
4.7	Wird über eine Plausibilitätsprüfung die Bewertung der Risiken überprüft?						
4.8	Ist definiert, dass die Risikoanalyse nicht nur durch eine einfache Addition von Schadenshöhen erfolgt?						
4.9	Werden bei Anwendung von Meldeschwellen zur lokalen Analyse vergleichbare und einheitliche Methoden verwendet?						
4.10	Sind die Meldeschwellen angemessen?						
4.11	Sind die potentiellen Ursachen der Risiken vollständig und plausibel beschrieben?						
4.12	Sind alle potentiellen und wesentlichen Auswirkungen in voller Bandbreite und nachvollziehbar beschrieben?						
4.13	Werden Korrelationen (Wechselwirkungen) von Risiken berücksichtigt, die zu einer Verstärkung oder Abschwächung der Auswirkungen führen können?						
4.14	Werden Risiken, die eingetreten sind bzw. deren Eintritt gewiss ist und die in die Unternehmensplanung bereits eingestellt sind, nicht mehr im Risikoportfolio aufgeführt?						
4.15	Ist sichergestellt, dass einmalige Risiken anders behandelt werden als permanente?						

5.0	**Risikosteuerung und -überwachung**						
5.1	Werden die Mitarbeiter zur permanenten Risikobewältigung sensibilisiert?						
5.2	Erfolgt bei der Risikobewältigung eine Konzentration auf die bestandsgefährdenden Risiken?						
5.3	Ist sichergestellt, dass auf Risiken zeitnah und wirkungsvoll reagiert werden kann?						
5.4	Erfolgt die Risikobewältigung bzw. Risikosteuerung nach nachvollziehbaren Kennzahlen (z.B. Ampelschaltung)?						
5.5	Sind die Kennziffern für die Risikosteuerung geeignet?						
5.6	Werden für die Maßnahmen zur Risikovermeidung bzw. -minderung Kosten/Nutzen-Analysen durchgeführt?						
5.7	Ist sichergestellt, dass eine permanente Anpassung der für die einzelnen Kennzahlen definierten Signale/Limite/Schwellenwerte bei Veränderungen erfolgt?						
6.0	**Risikoberichtserstattung und -kommunikation**						
6.1	Werden die wesentlichen Risiken regelmäßig an die Unternehmensleitung berichtet?						
6.2	Erfolgt je nach Adressat eine unterschiedlich umfangreiche Berichterstattung?						
6.3	Sind eindeutige Regelungen getroffen, wie und wer bei Erreichen eines Schwellenwertes aktiv wird?						

6.4	Gibt es für das Risikomanagement eine Organisations-Richtlinie und ein Handbuch bzw. Arbeitsanweisung?						
6.5	Erfolgt bei Veränderungen eine Anpassung dieser Dokumentationen?						
6.6	Gibt es eine einheitliche vorgegebene Bewertungsmethode und wird diese auf qualitative und quantitative Risiken gleich angewendet?						
6.7	Werden die richtigen Methoden richtig angewendet? (bspw. FMEA, Szenario-Analyse, Brainstorming, Workshops, Morphologische Matrix, Delphi-Methode etc.)						
6.8	Werden Risikobewertungen regelmäßig aktualisiert?						
6.9	Basieren quantitative Bewertungen auf geeigneten Wahrscheinlichkeitsverteilungen? (Bspw. Binomialverteilung, Dreipunktschätzung, Dreiecksverteilung, Gleichverteilung, kombinierte Verteilungen etc.?						
6.10	Sind die zugrunde gelegten Daten der quantitativen Bewertungen korrekt?						
6.11	Wie wird die Risikobewertung plausibilisiert?						
6.12	Sind Nettorisiken kleiner als Bruttorisiken?						
6.13	Sind die Nettorisiken korrekt auf Basis der Maßnahmen (z.B. Versicherung) ermittelt? (Wirkungsanalyse)						
6.14	Sind die Risiken aus verschiedenen Bereichen gleich bewertet worden, so dass eine Vergleichbarkeit besteht?						
6.15	Gibt es Kumulrisiken (Wechselwirkungen von Risiken)? Sind diese richtig/nachvollziehbar bewertet?						

6.16	Gibt es kompensierende Risiken? Sind diese richtig/nachvollziehbar bewertet?						
6.17	Gibt es Sekundärrisiken, die durch Maßnahmen das Risiko noch erhöhen?						
6.18	(Wie) wird ein Gesamtrisikoumfang des Unternehmens ermittelt? Werden Risikoerwartungswerte einfach addiert oder eine Risikoaggregation durchgeführt (z.B. mit einer Monte Carlo Simulation)?						

Autoren

Erarbeitet von der Fachgruppe Risikomanagement im DIIR-Arbeitskreis „Interne Revision im Mittelstand“:

Anja Erhardt
Arnd Furken CIA
Daniel Heinsen
Mohamed Kaddor
Dimitrios Karakidis CIA, CRMA
Rene Lange
Günther Meggeneder CIA, CRMA
Michael Neuy CISA, CIA, CISM, CRISC
Dieter Oskamp
Dr. Sylvia Waldner-Sander
Dieter Weise

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

Veröffentlicht im Dezember 2015 auf www.diir.de

Version 1.1