Positionspapier Interne Revision und Risikomanagement

Empfehlungen zum Zusammenwirken

Gemeinsames Positionspapier von DIIR und RMA

Version 2.0

RMA Risk Management & Rating Association e.V.

DIIR Deutsches Institut für Interne Revision e.V.

Inhalt

1 Präambel – Zielsetzung der Stellungnahme

Der Vorstand einer Aktiengesellschaft ist nach § 91 Abs. 2 AktG zur Einrichtung eines Überwachungssystems verpflichtet, um bestandsgefährdende Entwicklungen frühzeitig zu erkennen (Risikofrüherkennung). Mit dem am 01.01.2021 in Kraft getretenen Unternehmensstabilisierungs- und -restrukturierungsgesetz (StaRUG) wird ausdrücklich klargestellt, dass analog zu § 91 Abs. 2 AktG nun jede juristische Person, also auch die Geschäftsleitungen aller haftungsbeschränkten Gesellschaften (wie GmbHs und GmbH & Co. KGs), eine systematische Überwachung möglicher bestandsgefährdender Entwicklungen vorzunehmen haben. Fernerhin wurden die Anforderungen an das Risikomanagement aller haftungsbeschränkten Unternehmen präzisiert und erweitert. Bei einer Bestandsgefährdung wird nun von der Geschäftsleitung gefordert, „geeignete Gegenmaßnahmen“ der Krisen- und Risikobewältigung, erforderlichenfalls bis hin zu einem Restrukturierungsplan, zu ergreifen. Erkennt sie solche Risiken, ist sie verpflichtet, die Überwachungsorgane unverzüglich zu informieren (§ 1 Abs. 1 Satz 2 StaRUG).

Durch das am 01.07.2021 in Kraft getretene FISG (Gesetz zur Stärkung der Finanzmarktintegrität) wurden die Vorgaben des § 91 AktG mit Abs. 3 dahingehend ergänzt, dass der „Vorstand einer börsennotierten Gesellschaft darüber hinaus ein im Hinblick auf den Umfang der Geschäftstätigkeit und die Risikolage des Unternehmens angemessenes und wirksames internes Kontrollsystem und Risikomanagementsystem einzurichten“ hat. Ein den Anforderungen von § 91 AktG entsprechendes Risikomanagement umfasst neben dem Risikofrüherkennungssystem die Risikosteuerung bzw. Risikobewältigung sowie eine Risikoanalyse zur Vorbereitung „unternehmerischer Entscheidungen“ (§ 93 AktG). Die Einhaltung der (gesetzlichen) Anforderungen an die Angemessenheit und neuerdings auch an die Wirksamkeit des internen Kontrollsystems und des Risikomanagementsystems unterliegen nicht nur einer Prüfung durch die Abschlussprüfer. Die Prüfung stellt auch eine Kernaufgabe der Internen Revision dar und geht mit einem gesteigerten Prüfungsumfang sowie einer höheren Prüfungsintensität einher.

Der Aufsichtsrat hat nach § 107 Abs. 3 AktG die Wirksamkeit des internen Kontrollsystems, des Risikomanagementsystems und des internen Revisionssystems zu überwachen. Durch das FISG wurden die Vorgaben des AktG weitreichend ergänzt. So wurden u. a. die Zusammensetzung und Qualifikationen der Mitglieder des Aufsichtsrats (§ 100 Abs. 5 AktG) konkretisiert. Darüber hinaus wird mit dem neuen Abs. 4 des § 107 AktG erstmals neben der Verpflichtung zur Einrichtung eines Prüfungsausschusses für „Unternehmen von öffentlichem Interesse nach § 316a Satz 2 HGB” dem Vorsitzenden eines Prüfungsausschusses die gesetzlich verankerte Möglichkeit eingeräumt, direkt von den Leitungen, die für das interne Kontrollsystem, das Risikomanagementsystem oder die Interne Revision zuständig sind, Auskünfte einzuholen.

Diese erweiterten Anforderungen und die daraus erwachsenden Rechte und Pflichten schaffen allerdings in der Praxis vielfach Verunsicherung. Dies gilt insbesondere dort, wo sich Organisationsverschulden und persönliche Haftung auf die Organe der Unternehmen auswirken können. Die Art und Weise der genauen Ausgestaltung des Überwachungssystems und des Zusammenspiels der einzelnen Unternehmensfunktionen lässt der Gesetzgeber jedoch weitestgehend unbeantwortet.

Interne Revision und Risikomanagement sind wichtige Funktionen der Unternehmensführung und insbesondere des Überwachungssystems. Die Möglichkeiten des Zusammenwirkens dieser beiden wichtigen Unternehmensfunktionen stehen im Mittelpunkt dieses Positionspapiers. Denn aus der gesetzlichen Unbestimmtheit erwächst die Notwendigkeit, die Zusammenarbeit zwischen Interner Revision und Risikomanagement durch Empfehlungen der entsprechenden Fachverbände – Deutsches Institut für Interne Revision e.V. (DIIR) und RMA Risk Management & Rating Association e.V. (RMA) – praxistauglich aufzubereiten.

Mit dem „Three Lines Model“ (im Folgenden: 3LM) skizziert das Institute of Internal Auditors (IIA) ein Rahmenkonzept, bei dem die verschiedenen Funktionen des Überwachungssystems als modifizierte Rollenmodelle beschrieben werden. Hierzu betrachtet das IIA die Aufgaben des Leitungsorgans, des Managements, der risikorelevanten Überwachungsfunktionen, der Internen Revision und der externen Prüfer. Außerdem werden sechs Grundsätze für die neugefassten Rollen und Linien formuliert. Eine explizite Behandlung der Risikomanagementorganisation erfolgt dabei nicht.

Auch deshalb ist es aus fachlicher Sicht erforderlich, die unterschiedlichen Aufgaben von Interner Revision und Risikomanagement sowie die Möglichkeiten und Bedingungen ihres Zusammenwirkens zu konkretisieren. Dieses Positionspapier stellt verschiedene Organisationsformen mit ihren Vor- und Nachteilen dar und zeigt die daraus resultierenden Herausforderungen auf. Es wird zugleich verdeutlicht, dass neben der klaren aufbauorganisatorischen Trennung in der Praxis verschiedene Varianten und Kombinationsformen innerhalb des 3LM existieren, die unter bestimmten Voraussetzungen situationsgerecht und effektiv sein können.

Darüber hinaus gibt es in einigen Branchen besondere gesetzliche Anforderungen, z. B. im Gesundheitsbereich (z. B. Anforderungen an das Risikomanagement nach der europäischen Verordnung (EU) 2020/561 über Medizinprodukte, MDR) oder in der Finanzwirtschaft (MaRisk – Mindestanforderungen an das Risikomanagement), die jedoch in diesem Papier nicht betrachtet werden.

Die Stellungnahme wendet sich an diejenigen, die aufgrund rechtlicher Anforderungen zur Einrichtung, zum Betreiben und/oder zur Beaufsichtigung eines Überwachungssystems mit seinen Komponenten Risikomanagement- und Revisionssystem verpflichtet sind oder diese Systeme freiwillig einführen oder ausbauen wollen.

2 Aufgaben von Risikomanagement und Interner Revision

Bei der Analyse der Möglichkeiten zum Zusammenwirken von Risikomanagement und Interner Revision sind funktionelle und organisatorische Aspekte zu unterscheiden. Im 3LM des IIA werden beide Aspekte berührt, Schwerpunkt sind aber die Funktionsaspekte. Eine Funktion im Sinne von Aufgaben und Tätigkeiten kann von unterschiedlichen Personen und Abteilungen im Unternehmen wahrgenommen werden. Wenn diese Aufgaben und Tätigkeiten vollständig oder in wichtigen Teilbereichen auf eine Organisationseinheit übertragen werden, geht es um die institutionelle Verankerung, also um die Revisions- oder Risikomanagementabteilung und deren Zusammenwirken.

2.1 Funktion und Organisation von Risikomanagement und Interner Revision

Das Risikomanagement konzentriert sich auf Unternehmensziele und Ereignisse, die auf die Zielerreichung positiv oder negativ einwirken können. Diese Ausrichtung auf Chancen und Gefahren ist stärker mit der Beobachtung des externen Umfeldes verknüpft. Die Interne Revision arbeitet eher geschäftsprozessorientiert und überprüft Maßnahmen hinsichtlich Angemessenheit und Wirksamkeit, muss aber proaktiv auch die Risikoquellen des externen Umfelds im Blick haben.

Risikomanagement ist einerseits eine generelle unternehmerische Aufgabe und andererseits eine konkrete Aufforderung an das Unternehmen zur Gestaltung der Aufbau- und Ablauforganisation eines Risikomanagementsystems. Ziel ist die Gestaltung eines unternehmensweiten, integrierten und effektiven Risikomanagementsystems unter Berücksichtigung der unternehmensspezifischen Gegebenheiten. Gemäß den gängigen Risikomanagementstandards (ISO 31000 oder COSO ERM) soll das Risikomanagement alle wesentlichen Funktionen und operativen Bereiche im Unternehmen in den Analyseumfang einbeziehen („Risk Universe“). Das Risikomanagement ist somit Führungsaufgabe und Bestandteil aller Geschäftsprozesse, es muss aber zu seiner Wirksamkeit auch eine organisatorische Struktur haben.

Es empfiehlt sich daher, spezielle Abteilungen oder Personen mit organisatorischen Aspekten des Risikomanagements zu betrauen, auch wenn für das Management bestimmter Einzelrisiken die jeweiligen Führungskräfte als Risikoverantwortliche (Risk Owner) in der Pflicht

sind. Die jeweilige Aufgabenteilung bedarf einer kritischen Prüfung, die von der Unternehmensleitung, den Aufsichtsgremien sowie den externen Prüfern vorzunehmen ist. Für die Interne Revision ist die Prüfung des Risikomanagementsystems gemäß den Internationalen Standards für die berufliche Praxis des IIA eine Pflichtaufgabe.

Auch die **Interne Revision** kann als Funktion im Sinne einer durch Unternehmensangehörige durchgeführten Prüfungstätigkeit betrachtet werden. In der Regel ist sie in einer eigenen Abteilung institutionalisiert. Insofern sind ihr Vorhandensein und ihre Arbeit, wie alle anderen Unternehmensfunktionen auch, Gegenstand einer Risikobetrachtung, die in das Risikomanagementsystem einzubeziehen ist. Das gilt besonders auch dann, wenn eine Revisionsabteilung nicht vorhanden ist.

Andererseits gehört es zu den Aufgaben der Internen Revision, die Angemessenheit und Wirksamkeit des Risikomanagements im Ganzen oder im Einzelfall zu überprüfen. Gemäß dem DIIR-Revisionsstandard Nr. 2 gehört zur Funktionsfähigkeit, dass:

- wesentliche Risiken erkannt und bewertet werden,
- angemessene Risikomaßnahmen, die mit der Risikoakzeptanz der Organisation im Einklang stehen, ergriffen werden und
- wesentliche risikobezogene Informationen erfasst und rechtzeitig in der Organisation kommuniziert werden, sodass es Mitarbeitenden, Führungskräften und Geschäftsleitung bzw. Überwachungsorgan möglich ist, ihren Verantwortlichkeiten gerecht zu werden.

Bei der Prüfung des Risikomanagementsystems ergeben sich umfangreiche Prüfungserfordernisse, die sowohl die Abschlussprüfer als auch die Interne Revision betreffen. Dabei ist eine Zusammenarbeit zwischen Interner Revision und Abschlussprüfern ausdrücklich gewünscht. Es ist aber zu beachten, dass die Abschlussprüfer bisher mit dem IDW-Prüfungsstandard 340 n.F. (2020) lediglich die gesetzlichen Anforderungen an das Risikofrüherkennungssystem nach § 91 Abs. 2 AktG untersuchen. Aus § 93 AktG und § 1 StaRUG sowie dem FISG ergeben sich jedoch erweiterte Anforderungen an das Risikomanagement, die auch Gegenstand einer Prüfung durch die Interne Revision sein müssen.

Die Prüfung des Risikomanagements nach DIIR Revisionsstandard Nr. 2 geht über eine Prüfung durch den Abschlussprüfer nach IDW PS 340 und IDW PS 981 hinaus. Bei den börsennotierten Aktiengesellschaften ist auch durch die Interne Revision zu prüfen, ob nicht nur ein umfassendes und angemessenes, sondern auch ein wirksames Risikomanagement existiert (§ 91 Abs. 3 AktG).

Die praktische Umsetzung einer Prüfung des Risikomanagementsystems erleichtert der DIIR Revisionsstandard Nr. 2 in Verbindung mit dem Prüfungsleitfaden in Form eines Tools,

den der gemeinsame DIIR-RMA-Arbeitskreis „Interne Revision und Risikomanagement“ entwickelt hat.[1]

Zu ergänzen ist, dass die Interne Revision nicht nur Bestandteil des internen Überwachungssystems ist, sondern auch die Prozesse der anderen Überwachungsfunktionen, neben dem Risikomanagement zum Beispiel Compliance, Controlling, Qualitätsmanagement und das interne Kontrollsystem, in ihre Prüfungstätigkeiten einzubeziehen hat.

Für die Organisation der Internen Revision gelten besondere Maßstäbe. Sie betreffen vor allem die Unabhängigkeit dieser Abteilung. Gemäß den Internationalen Standards bedeutet Unabhängigkeit, dass keine Umstände vorliegen, die die Fähigkeit der Internen Revision beeinträchtigen, ihre Aufgaben unbeeinflusst wahrzunehmen. Zusätzlich muss die Leitung der Internen Revision direkten und unbeschränkten Zugang zur Geschäftsleitung und ggf. zum Überwachungsorgan haben.

2.2 Methodische Gemeinsamkeiten und Unterschiede

Ein methodischer Unterschied besteht darin, dass bei einer Prüfung durch die Revision die tatsächlichen Schwachstellen bzw. mögliche Optimierungspotenziale im Vordergrund stehen, die in der Praxis häufig qualitativ bewertet werden, im Risikomanagement hingegen eine quantifizierte Einschätzung von Risikopotenzialen erfolgt. So impliziert nicht zuletzt das StaRUG für das Risikomanagement die Notwendigkeit zur Messung „bestandsgefährdender Entwicklungen” im Kontext eines Risikofrüherkennungssystems. Da jedoch bestandsgefährdende Entwicklungen in der Regel durch Kombinationseffekte mehrerer Risiken hervorgerufen werden, ist eine quantitative Bewertung von Risiken mit Blick auf Liquidität und Eigenkapital oder EBIT und Verschuldungsgrad sowie eine Aggregation zum Gesamtrisiko unabdingbar, um die Risikotragfähigkeit des Unternehmens zu bestimmen. Folglich ist eine Gesamtschau der möglichen Risiken eines Unternehmens oder einer Unternehmensgruppe in der Regel dem Risikomanagement vorbehalten und erfolgt nicht durch die Revision.

Auch in der Arbeitsplanung und -durchführung bestehen Unterschiede. Das Risikomanagement arbeitet, abgesehen von Ad-hoc-Meldungen, in einem zyklischen Prozess, bei dem in der Regel mindestens einmal jährlich eine Risikoinventur mit anschließender Risikobewer-

[1] Abrufbar unter www.diir.de oder www.rma-ev.org.

tung vorgenommen wird. Die Interne Revision geht bei ihrer Prüfungstätigkeit von einer risikoorientierten, mindestens jährlich erstellten Planung aus, die durch ungeplante, aus gegebenem Anlass entstehende Prüfungen ergänzt werden kann. Beide Funktionen müssen die zunehmende Unsicherheit und Komplexität unternehmerischer Entscheidungen beachten. Typisch für die Arbeit der Internen Revision sind die intensive Vor- und Nachbereitung der einzelnen Prüfungen und die Prüfungsdurchführung vor Ort. Aber auch das Risikomanagement arbeitet projektbezogen, wenn seine Expertise, z. B. bei der Beurteilung großer Unternehmensinvestitionen und Akquisitionen, gefragt ist. Bei der Bearbeitung von Risikosteuerungs- und Verbesserungsmaßnahmen, sei es zur Minderung der festgestellten Risiken oder zur Mängelbeseitigung gemäß Revisionsbericht, ergeben sich wiederum Gemeinsamkeiten in der Nachverfolgung (Follow-up).

3 Anforderungen an die Zusammenarbeit

Voraussetzung für eine funktionierende Zusammenarbeit ist eine klare und eindeutige Definition der Begriffe und der Aufgabengebiete der beiden Abteilungen. Dies ist erforderlich, um Doppelarbeiten zu vermeiden, berufsständische Standards einzuhalten und knappe Ressourcen wirksam innerhalb der Organisation einzusetzen.

3.1 Vereinheitlichung der Begriffe und Abgrenzungen, Berichtswesen

Generell werden die Kommunikation und der Austausch über Risiken im Unternehmen vereinfacht, wenn gleiche Begrifflichkeiten, Organisationsbezeichnungen, Risikokategorien und Risikobewertungssysteme verwendet werden. Bei der Benennung der Prüfungsobjekte für Zwecke der Revision und der Risikokategorien und Bereiche im Risikomanagement sollten sich daher die Organisationszuständigen fortlaufend abstimmen.

Eine vollständige Deckungsgleichheit wird in der Regel nicht herstellbar sein. Abweichungen zwischen Revision und Risikomanagement können sich z. B. dann ergeben, wenn die Revision rechtliche Einheiten, beispielsweise Tochtergesellschaften, als Risiko- und Prüfobjekt festlegt und dazu bestimmte Funktionsbereiche wie Rechnungswesen, Logistik, Einkauf, Vertrieb, IT oder Personal oder auch bestimmte Geschäftsprozesse auswählt.

Das Risikomanagement definiert die Risikoeinheiten häufig entsprechend der Management-Reporting-Struktur oder, wie im Geschäfts-/Lagebericht dargestellt, auf Basis produkt- oder dienstleistungsorientiert definierter Geschäftseinheiten. Zusätzlich können im Risikomanagement Aspekte wie Kundengruppen, Produktgruppen, Material- und Lieferantengruppen und die verschiedenen Anspruchsgruppen (Stakeholder) Berücksichtigung finden.

Unterschiede in der Strukturierung der Prüfungs- und Risikoeinheiten wirken sich auch im Berichtswesen aus. Beide Funktionen haben in der Regel sowohl in der Form als auch im Adressatenkreis bereits etablierte Berichte. Eine Harmonisierung des Berichtswesens wäre zwar im Sinne der Berichtsempfänger wünschenswert, eine getrennte Berichterstattung von Revision und Risikomanagement kann, z. B. aus Gründen der Vertraulichkeit oder spezifischer Berichtsinhalte, erforderlich sein. Da teilweise zu gleichen Themen berichtet wird, empfiehlt sich eine Abstimmung und gegenseitige Information über die jeweiligen Berichtsinhalte.

3.2 Kommunikation und Informationsaustausch

3.2.1 Auskunftsrechte und -pflichten sowie Kommunikationswege

Zwischen Revision und Risikomanagement ist ein direkter und bei Bedarf auch von beiden Seiten kurzfristig nutzbarer Kommunikationsweg sicherzustellen. Die Revision benötigt für die Wirksamkeit ihrer Arbeit den Zugang zu allen relevanten Informationen im Unternehmen. Ob dieses uneingeschränkte Einsichtsrecht auf Anfrage oder durch permanente Leserechte, z. B. in Risikodatenbanken, erfolgt, ist unternehmensspezifisch abzuwägen. Die Interne Revision sollte routinemäßig in den Verteiler der vom Risikomanagement erstellten Berichte einbezogen werden.

Die Informationsweitergabe der Revision an das Risikomanagement kann auf unterschiedliche Art erfolgen:

- systematischer vollständiger Austausch von Revisionsberichten, ggf. mit Einschränkungen bei Sonderthemen mit personenbezogenen Daten, oder
- systematischer themenbezogener Austausch von Informationen durch Weitergabe relevanter Teilauszüge von Revisionsberichten.

Zur Vermeidung einer Überfrachtung mit Informationen sollten beide Seiten vorab definieren, welche Informationen sie tatsächlich benötigen.

Bei Revisionen erkannte Risiken sollten zeitnah mit dem Risikomanagement ausgetauscht und gegebenenfalls ausführlich diskutiert werden.

3.2.2 Zeitpunkt, Häufigkeit und Inhalte des Austauschs

Die Teilnahme der Revision an Sitzungen von Risikomanagement-Gremien und die Möglichkeit zur Beteiligung an der Diskussion risikorelevanter Themen ist anzustreben. Der Rhythmus des Austauschs kann dabei variieren:

- regelmäßig, z. B. vor Prüfungsausschusssitzungen, insbesondere wenn alle Einheiten separat berichten,
- ad hoc zu besonderen Risikosituationen, z. B. in Projekten, bei veränderten Umweltbedingungen oder aktuellen Vorkommnissen, bei politischen oder rechtlichen Besonderheiten oder Änderungen,
- ereignisgetrieben, z. B. bei M&A-Entscheidungen und Due-Diligence-Untersuchungen.

Inhalt des Austauschs sollten auch die Prüfungspläne der Revision sowie weitere geplante Aktivitäten und Projekte beider Seiten sein. Ebenso sollte man sich über Veränderungen in der Risikolage, Systemanpassungen oder auch veränderte Methoden in der Arbeit der Abteilungen austauschen. Insbesondere im Zuge der Aufstellung des Revisionsplans ist durch die Interne Revision eine Diskussion der Risikosituation mit dem Risikomanagement anzustreben.

Ein solcher regelmäßiger Informationsaustausch zwischen Revision und Risikomanagement dient zur Sicherstellung eines funktionierenden Überwachungssystems. Die Revision profitiert bei der Ausrichtung der risikoorientierten Prüfungsstrategie/-planung vom Informationsaustausch mit dem Risikomanagement. Das Risikomanagement kann durch die Interne Revision wichtige Hinweise zur Verbesserung des Risikomanagementsystems, z. B. zu bestehenden Regelungen und Maßnahmen, sowie zur frühzeitigen Identifikation neuer wesentlicher Risiken erhalten.

4 Organisationsformen der Internen Revision

In diesem Kapitel geht es um die Organisationsform der Internen Revision. Mögliche Organisationsformen eines eigenständigen Risikomanagements werden hier nicht betrachtet, da es dafür keine externen Vorgaben gibt. Ausgehend vom 3LM des IIA werden mögliche Varianten (Mischmodelle) und deren Begleitumstände erörtert. Damit soll auch der Tatsache Rechnung getragen werden, dass in der deutschen Unternehmenspraxis Mischmodelle stark verbreitet sind.

Eine Funktionserweiterung ist nach den Internationalen Standards des IIA grundsätzlich zulässig, wenn durch geeignete Vorkehrungen der Geschäftsleitung bzw. des Überwachungsorgans Unabhängigkeit und Objektivität der Internen Revision sichergestellt werden. Das IIA geht in den Leitlinien zum Standard 1112 auf die möglichen Zusatzfunktionen und die dazu geeigneten Vorkehrungen zur Sicherstellung der Unabhängigkeit der Revisionsfunktion ein, wie zum Beispiel eine zeitliche Begrenzung der zusätzlichen Aufgaben oder das Beauftragen alternativer, unabhängiger Prüfungen.[2] Auf einige weitere Maßnahmen wird weiter unten eingegangen.

Auch im 3LM des IIA wird auf die mögliche Übernahme zusätzlicher Entscheidungsverantwortung der Revisionsleitung für verwandte Aufgaben hingewiesen.[3]

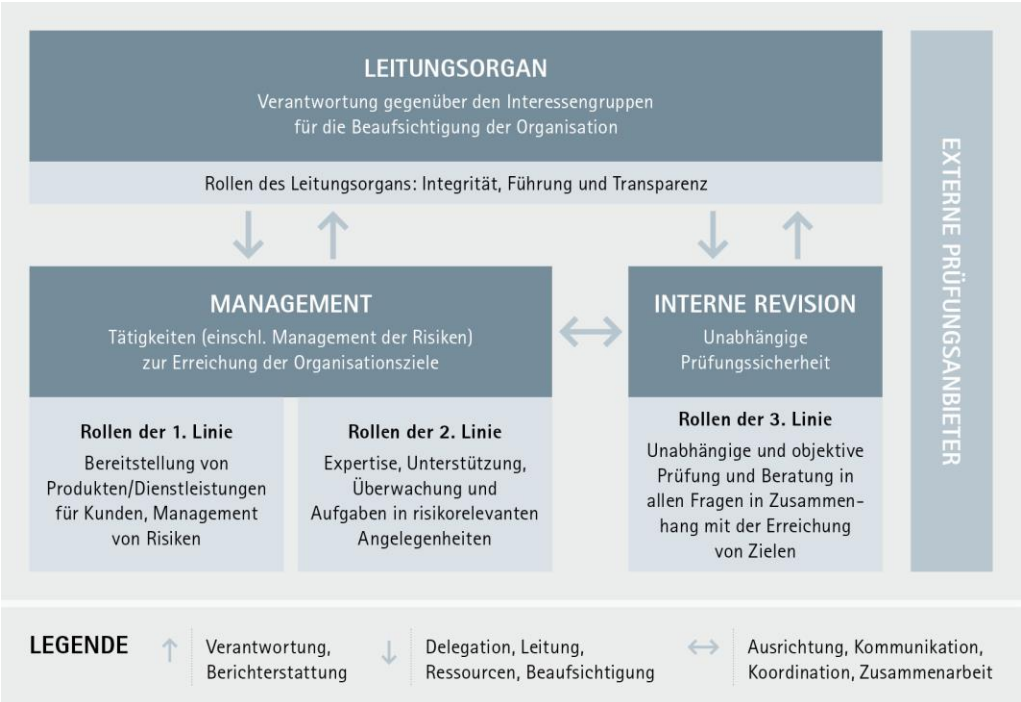
[2] Implementierungsleitlinie zum Standard 1112 im Rahmen der Internationalen Grundlagen für die berufliche Praxis der Internen Revision.

[3] Das Drei-Linien-Modell des IAA, S.3, Fn. 3: „In manchen Organisationen werden andere Rollen der dritten Linie benannt, wie z. B. Beaufsichtigung, Inspektion, Ermittlung, Bewertung und Sanierung. Diese können Teil der internen Revisionsfunktion sein oder separat agieren."

4.1 Interne Revision und Drei-Linien-Modell

4.1.1 Konzeption des Drei-Linien-Modells

Bereits in der Präambel dieses Positionspapiers wurde darauf hingewiesen, dass das bisherige „Three Lines of Defense Model“ vom IIA durch das 3LM ersetzt wurde. Das 3LM dient als Veranschaulichung eines funktionsfähigen und wirksamen Steuerungs- und Überwachungssystems in Unternehmen, welches insbesondere die Unabhängigkeit der Internen Revision und die Notwendigkeit der Kommunikation, Kooperation und Koordination zwischen den Funktionen hervorhebt. Neben den drei Linien operatives Management, Unterstützungsfunktionen des Managements und Interne Revision berücksichtigt dieses Modell auch die Rolle des Leitungsorgans und der externen Prüfungsanbieter. Die nachfolgende Abbildung zeigt die Zuordnung der verschiedenen Rollen und Aufgaben.



Im oberen Teil der Darstellung ist das Leitungsorgan eingezeichnet. Im deutschen Rechtsraum umfasst dies das Aufsichtsorgan und die Geschäftsleitung, z. B. den Aufsichtsrat und den Vorstand. Ihm sind unter anderem die Überwachungsfunktionen (Governance) einschließlich Risikofrüherkennung und Interner Revision zugeordnet.

Die erste Linie ist darauf ausgerichtet, dem internen und externen Kunden Produkte und/oder Dienstleistungen zu liefern, und umfasst die Rollen von Unterstützungsfunktionen wie

Personal, Verwaltung, IT und Gebäudeservice. Zur ersten Linie gehört auch die operative Verantwortung für das Management von Risiken.

Die Rollen der zweiten Linie sind solche, die sich auf Aufgaben in risikorelevanten Bereichen beziehen. Das ist nicht nur das Risikomanagement selbst, sondern sind auch Funktionen wie Compliance, Arbeitsschutz, Datenschutz, Umweltschutz und Nachhaltigkeit sowie Internes Kontrollsystem.

Die dritte Linie ist die Revisionsfunktion. Sie ist unabhängig vom Management und dessen Verantwortlichkeiten. Diese Unabhängigkeit gewährleistet eine objektive Prüfungssicherheit und Beratung.

Das IIA betont in seinem Papier: „Das Leitungsorgan, das Management und die Interne Revision haben ihre unterschiedlichen Verantwortlichkeiten, aber alle Aktivitäten müssen auf die Ziele der Organisation abgestimmt sein. Die Grundlage für ein erfolgreiches Zusammenwirken ist eine regelmäßige und wirksame Koordination, Zusammenarbeit und Kommunikation.“[4]

4.1.2 Vor- und Nachteile einer strikten Trennung von Risikomanagement und Revision

Eine strikte organisatorische Trennung von Risikomanagement und Revision bietet den Vorteil der Klarheit hinsichtlich der Verantwortlichkeit im internen Überwachungssystem für alle Beteiligten: Das Risikomanagement unterstützt und überwacht die Funktionen der ersten und zweiten Linie, ausgenommen sich selbst. Die Interne Revision prüft sämtliche Komponenten der ersten und zweiten Linie. Dabei ist die Revisionsleitung aufgrund der klaren Trennung unabhängig und ist einem eher geringen Risiko von Interessenkonflikten ausgesetzt.

Nachteile einer solchen strikten Trennung der Funktionen können darin liegen, dass die Organisation durch Doppelarbeiten unnötig belastet wird (z. B. Durchführung von Risikoanalysen, ähnlich gelagerte Analysen und Prüfungen). Diese möglichen Nachteile sind durch eine enge methodische Abstimmung und intensive Kommunikation zwischen den Funktionen zu minimieren. Darauf sollte auch die Unternehmensleitung achten und dies von den Funktionsverantwortlichen einfordern. Nicht zuletzt könnte ein Nachteil dieser Organisation im größeren Ressourcenbedarf der auszustattenden Überwachungsfunktionen bestehen.

[4] Das Drei-Linien-Modell des IIA, S. 8.

4.1.3 Unterschiedliche Fokussierung der Internen Revision

Das Verständnis der eigenen Überwachungsaufgaben ist nicht nur in verschiedenen Unternehmen, sondern auch innerhalb der Unternehmen in den verschiedenen Bereichen der zweiten Linie oft unterschiedlich ausgeprägt. In Abhängigkeit davon gestaltet sich auch die Arbeit der dritten Linie unterschiedlich.

Fokussieren sich die zweite Linie und deren Vertreter tendenziell auf die Vorgabe von Regelungen oder die Gestaltung von Managementsystemen und weniger auf die Überwachung, ob die Regelungen im Unternehmen eingehalten werden, dann wird die Revisionsarbeit sich stärker auf die Prüfung der ersten Linie konzentrieren müssen, um eine Aussage zur Funktionsfähigkeit von Systemen oder der tatsächlichen Implementierung von Vorgaben treffen zu können. Dies gilt für die praktische Umsetzung der Vorgaben des Risikomanagements wie für andere Funktionen und deren Anforderungen, zum Beispiel Compliance oder den Bereich Safety, Health, Environment, Quality (SHEQ).

Je mehr die zweite Linie Überwachungsaufgaben ausübt, um sich von der Einhaltung von Regeln zu überzeugen, desto stärker können sich die Revisionsaufgaben auf die Prüfung der zweiten Linie ausrichten, insbesondere wie diese die Funktionsfähigkeit und Regeleinhaltung sicherstellt. Diese Modellausprägung mit einer eher überwachenden Risikomanagementfunktion stärkt insgesamt die Sicherheit im Unternehmen, erfordert im Gegenzug jedoch entsprechende Kompetenzen und Ressourcen in der zweiten Linie. Diese Ressourcen können entweder aufgebaut oder mit externer Unterstützung bereitgestellt werden. Es hängt von den Erwartungen der Unternehmensführung an die Ausgestaltung des Risikomanagementsystems und andere Funktionen ab, inwieweit die zweite Linie nur gestalterisch oder auch überwachend tätig wird.

Mit Blick auf das Risikomanagement wird der Prüfungsfokus der Internen Revision nicht unerheblich vom Reifegrad des Risikomanagements bestimmt. Ist unter anderem die Risikomanagementfunktion noch nicht sehr stark entwickelt bzw. gar nicht vorhanden, so muss sich der Prüfungsfokus der Revision dahin verschieben, dass sie auf diesen Mangel hinweist und prüft, wie die Unternehmensrisiken von anderen vorhandenen Managementfunktionen, insbesondere vom Controlling, erfasst werden können. Ein zentrales Prüfungsergebnis kann die Empfehlung zur Einführung und Organisation von adäquaten Risikomanagementprozessen sein. Erst ein ausgereiftes und vollständig implementiertes Überwachungssystem im Sinne des 3LM stellt sicher, dass alle Risiken systematisch gesteuert werden und die unternehmensinterne Risikokommunikation gewährleistet ist. Bei voll ausgereiften Funktionen der zweiten Linie steht dann folgerichtig für die Revision eher die Prüfung der Wirksamkeit des Risikomanagementsystems sowie der Kommunikationswege im Vordergrund.

4.2 Merkmale der Mischformen

4.2.1 Vor- und Nachteile einer Kombinationsform von Risikomanagement und Revision

Die Vorteile einer Kombinationsform von Risikomanagement und Revision liegen in der integrierten Betrachtung des Unternehmensumfelds. Dies kann zu einer systematischeren Nutzung aller Risikoinformationen führen und den methodischen Reifegrad erhöhen. Die in Kapitel 3 aufgeführten Anforderungen an die Zusammenarbeit von Risikomanagement und Interner Revision lassen sich leichter umsetzen, wenn eine enge organisatorische Verbindung beider Funktionen besteht. Hinzu kommen die produktive Ergänzung der verschiedenen Sichtweisen und die verbreiterten Arbeitskontakte in das Unternehmen. Auch kann eine solche Kombinationsform Kostenvorteile haben.

Dem gegenüber stehen mögliche Einschränkungen der Unabhängigkeit oder des Umfangs der Revisionstätigkeit, denn in den Gebieten, in denen die Interne Revision selbst operative Aufgaben übernimmt, kann sie keine unabhängige Prüfung vornehmen. Außerdem kann es schwierig sein, Prioritäten zu setzen. Diese lassen sich nur in Grenzen grundsätzlich festlegen, sodass für das Management ein höherer Koordinationsaufwand entstehen kann.

4.2.2 Unterschiedliche Integrationsumfänge

Die grundsätzliche Prioritätsfrage kann durch unterschiedliche Abstufungen der Funktionsintegration pragmatisch beantwortet werden. Es gibt dazu zwei Varianten, die im Einzelnen weiter differenziert werden können. Die nachfolgenden Ausführungen gehen dabei davon aus, dass die Revision zusätzliche Aufgaben übernimmt. Das schließt nicht aus, dass auch umgekehrte Organisationsansätze mit Ausgangspunkt Risikomanagement in der Praxis anzutreffen sind.

Vollintegration – die Revision übernimmt Aufgaben der Gestaltung des Risikomanagementsystems und Verantwortung für die Prozesse des Risikomanagements

Bei der Vollintegration übernimmt die Revision Aufgaben, die gemäß der Definition im 3LM der zweiten Linie (Systemgestaltung und Risikomanagementprozesse) zuzuordnen sind. Eine eigenständige Risikomanagementfunktion existiert in diesem Fall also nicht. Die Revision wird damit Teil des Systems, das sie eigentlich überwachen soll. Hinsichtlich des Risikomanagements bedeutet eine Vollintegration neben der Übernahme der Systemdefinition auch die Sicherstellung einer angemessenen Risikoidentifikation, der Risikobewertung und das organisatorische Management der Risikosteuerung durch die Revision selbst. Deshalb

steht der Vollintegration der Grundsatz der Unabhängigkeit der Revision entgegen – für die Revision entsteht ein Interessenkonflikt. Sie kann die Wirksamkeit des Risikomanagementsystems nicht prüfen. Eine solche Prüfung muss durch einen externen, unabhängigen Prüfungsdienstleister im Auftrag und unter Aufsicht des Leitungsorgans durchgeführt werden.

Teilintegration – die Revision übernimmt Aufgaben der Systemgestaltung mit Wirksamkeitsprüfung

Im Gegensatz zur Vollintegration übernimmt die Revision bei der Teilintegration ebenfalls Aufgaben der zweiten Linie, aber nur in der Systemgestaltung. Diese systemischen Vorgaben werden dann – getrennt von der Revision – durch die operativen Einheiten der ersten Linie umgesetzt. Auch hier existiert organisatorisch und personell keine separate Risikomanagementfunktion. Für das Risikomanagement bedeutet dies, dass die Revision die Grundsätze und die Vorgehensweise im Risikomanagement vorgibt (Systemdefinition). Die operativen Einheiten wiederum setzen diese Vorgaben um, indem sie ihre operativen Risiken eigenständig identifizieren, bewerten und Bewältigungsmaßnahmen umsetzen und darüber berichten. Die Wirksamkeitsprüfung der operativen Umsetzung der Risikomanagementaufgaben kann dann von der Revision als klassische Aufgabe der dritten Linie unabhängig wahrgenommen werden, da sie anders als bei der Vollintegration daran nicht unmittelbar beteiligt ist. Hingegen kann sie die Gestaltung des Risikomanagementsystems (Angemessenheit) nicht unabhängig prüfen.

4.2.3 Weitere Mischmodelle zur Überwachung des Unternehmens

Dieses Positionspapier befasst sich in erster Linie mit der Positionierung von Risikomanagement und Revision im Unternehmen. Dabei darf nicht außer Acht gelassen werden, dass in der Praxis auch weitere Kombinationsformen bestehen, beispielsweise unter Einbeziehung von Aufgaben der Compliance. Faktisch haben sich in der Unternehmenswelt diverse Kombinationen mit und ohne Beteiligung der Internen Revision etabliert, da durch auf die jeweilige Situation zugeschnittene Organisationsformen Effizienz- und Effektivitätsvorteile erwartet werden.

Weitere in der Praxis anzutreffende Beispiele sind Kombinationsformen, bei denen auch technische Funktionen (z. B. Qualitätsmanagement) oder spezielle Überwachungsfunktionen (z. B. Geldwäschebeauftragte, Ombudsleute oder Umweltbeauftragte) unterschiedlichen Funktionsbereichen zugeordnet werden.

4.2.4 Interessenkonflikte in Mischformen

Interessenkonflikte treten immer dann auf, wenn die Revision neben ihrer Prüfungstätigkeit gestalterische und operative Funktionen übernimmt. Der Interessenkonflikt besteht darin, dass es dann zu Situationen einer Selbstprüfung kommen würde. Die Beeinträchtigung der Unabhängigkeit gefährdet in diesen Fällen die Objektivität der Prüfung. In diesen Fällen ginge die Verantwortung der Revision über die dritte Linie hinaus.

In Mischformen ergeben sich Einschränkungen für die Unabhängigkeit der Internen Revision. Diese Einschränkungen unterscheiden sich in ihrer Ausprägung je nach Integrationsgrad, Organisationsform oder Führungsmodell. Entsprechend sind bei Mischformen neben deren Vor- und Nachteilen stets auch die folgenden Fragen zur Verringerung von Interessenkonflikten zu diskutieren:

- Welche konkreten Aufgaben sollen durch die Revision zusätzlich übernommen werden?
- Welche operativen, administrativen, unternehmerischen und haftungsreduzierenden Vorteile und Kostenersparnisse ergeben sich aus der beabsichtigten Mischform?
- Wie ist diese Multifunktionalität organisatorisch abzubilden (Zuordnung, Berichtswege, Rechte und Pflichten)?
- Welche interne oder externe Institution kann an Stelle der Revision eine unabhängige Prüfung der betroffenen Mischfunktionen unter Beaufsichtigung der Geschäftsleitung oder des Aufsichtsorgans vornehmen (Wirtschaftsprüfer, externer Auditor)?
- Welche Lösungswege sind bei möglichen Interessenkonflikten vorgesehen?

Die dazu gewählten Antworten könnten dann mit folgenden Maßnahmen begleitet werden:

- Gemeinsame Darstellung der Tätigkeiten von Revision und Risikomanagement bzw. sonstiger Funktionen in einer Organisationsbeschreibung.
- Benennung von Art und Umfang der durch andere externe oder interne Stellen zu prüfenden Bereiche.
- Definition von Indikatoren, die eine Beurteilung der Wirksamkeit des Risikomanagements und anderer Funktionen durch das verantwortliche Management selbst erlauben, z B. Backtesting-Fragen wie: Sind die Risiko-Prognosen zutreffend gewesen?

In der Implementierungsleitlinie zum Standard 1112 des IIA finden sich Empfehlungen zur Sicherstellung einer objektiven Prüfung, die hier auszugsweise wiedergegeben werden:

- Klarstellung der Objektivitätsverpflichtung in Richtlinien und im Ethikkodex der Organisation, in der Geschäftsordnung des Prüfungsausschusses, in der Deklaration der Unternehmenspolitik, in der Geschäftsordnung der Revision, in der Beschreibung der Verantwortlichkeiten der Leitung der Revision.

- Die Dokumentation der Protokolle von Sitzungen der Geschäftsleitung bzw. des Überwachungsorgans, in denen die Leitung der Revision potenzielle Beeinträchtigungen von Unabhängigkeit und Objektivität offenlegt und Sicherungsmaßnahmen vorschlägt.
- Die Aufnahme der Hauptthemen des Risikomanagements in die Jahresberichterstattung der Revision, da Themen, die dort enthalten sind, durch Vorstand und externe Wirtschaftsprüfer zur Kenntnis genommen werden.
- Nachweise können auch in Form von Umfragen unter den Revisionskunden und Bewertungen durch die Geschäftsführung bzw. das Überwachungsorgan in Bezug auf die wahrgenommene Unabhängigkeit und Objektivität der Leitung der Revision erfolgen.
- Die Einhaltung kann auch anhand der Ergebnisse von externen Beurteilungen durch einen unabhängigen Beurteiler validiert werden.

Der Prüfungsausschuss einer Aktiengesellschaft hat u. a. die Wirksamkeit des Revisionssystems festzustellen (§ 107 Abs. 3 AktG). Daher wäre die Umsetzung einer Mischform mit dem Prüfungsausschuss oder dem Beirat bzw. den Gesellschaftern abzustimmen und auch vom Vorstand formal zu genehmigen. In öffentlich-rechtlichen Organisationen empfiehlt sich die Abstimmung der Mischform mit den jeweiligen Verwaltungsräten oder Beiräten bzw. mit den Kommunalvertretungen. Soll dabei nicht gegen die Internationalen Standards für die berufliche Praxis der Internen Revision verstoßen werden, so ist die Prüfungsfunktion für den die Unabhängigkeit der Internen Revision beeinträchtigenden Bereich an einen externen und unabhängigen Prüfungsdienstleister zu vergeben. Daraus resultierende Kosten sind in einer Gesamtbewertung der organisatorischen Effizienz zu berücksichtigen.

5 Fazit

Die Umsetzung des 3LM in einer Mischform ist rechtlich zulässig, soweit dem nicht regulatorische Vorgaben für einzelne Branchen entgegenstehen. Sie kann in Teilbereichen zu einem Verlust an Unabhängigkeit der Internen Revision und potenziell zu einer Abweichung von den Internationalen Standards führen. Dies kann aber z. B. durch die Einschaltung externer, unabhängiger Prüfungsdienstleister kompensiert werden.

Andererseits können sich durch die Integration von Funktionen der Revision mit anderen Funktionen und eine bewusste Aufhebung der Trennung zwischen den Aufgaben der zweiten und dritten Linie neben Effizienzvorteilen bei der Systemgestaltung und Systemüberwachung auch Vorteile für den unternehmerischen Erfolg der Organisation ergeben.

Die Geschäftsleitungen und Aufsichtsorgane der Unternehmen sollten ihre Entscheidungsfreiheit verantwortungsvoll und mit Blick auf die spezifischen Gegebenheiten des Unternehmens wahrnehmen. Bevor bestimmte Rein- oder Mischformen ausgewählt werden, ist vor allem sicherzustellen, dass Risikomanagement und Revisionsaufgaben einen angemessenen Stellenwert im Unternehmen haben.

Autoren

Das Positionspapier wurde im gemeinsamen Arbeitskreis „Interne Revision und Risikomanagement“ von DIIR – Deutsches Institut für Interne Revision e.V. und RMA Risk Management & Rating Association e.V. erarbeitet.

Mitglieder der Arbeitsgruppe waren Jens Diegel (CIA, CRMA), Oliver Disch, Eberhard Graf, Martin Gutzmer (CIA), Dr. Michael Hadaschik, Dr. Andreas Kempf (CRMA), Ralf Kimpel (CIA, CRMA), Gunnar Krause, Jörg Uffelmann und Prof. Dr. Gabriele Wieczorek.

In der Version 2.0 veröffentlicht am 31.10.2022 auf www.diir.de und www.rma-ev.org.

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

RMA Risk Management & Rating Association e.V.
Zeppelinstraße 73
81669 München