Positionspapier Interne Revision und Risikomanagement

Empfehlungen zum Zusammenwirken

Gemeinsames Positionspapier von DIIR und RMA

Version 1.0

RMA Risk Management & Rating Association e.V.

DIIR Deutsches Institut für Interne Revision e.V.

Inhalt

1 Präambel – Zielsetzung der Stellungnahme

Der Vorstand ist nach § 91 Abs. 2 AktG gesetzlich zur Einrichtung eines Überwachungssystems verpflichtet, um bestandsgefährdende Entwicklungen rechtzeitig zu erkennen (Risikofrüherkennung). Der Aufsichtsrat hat nach § 107 Abs. 3 AktG die Wirksamkeit des Risikomanagementsystems zu überwachen. Für Geschäftsführer und Aufsichtsorgane einer GmbH ergeben sich diese Pflichten analog aufgrund der Ausstrahlungswirkung dieser aktienrechtlichen Regelungen zum Risikomanagement.

Diese 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 Frage nach der organisatorischen Ausgestaltung stellt sich darüber hinaus auch für alle Organisationen außerhalb von Kapitalgesellschaften immer, wenn die Zusammenarbeit bzw. die Abgrenzung von Revisionsfunktion und Risikomanagement zu klären ist.

Die Frage der genauen Ausgestaltung des Überwachungssystems und des Zusammenspiels der einzelnen Unternehmensfunktionen lässt der Gesetzgeber weitestgehend unbeantwortet. Interne Revision und Risikomanagement sind wichtige Funktionen der Unternehmensführung und insbesondere des Überwachungssystems. Die Frage des Zusammenwirkens dieser beiden wichtigen Unternehmensfunktionen steht im Mittelpunkt der vorliegenden Stellungnahme.

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) – unternehmensadäquat zu gestalten.

Darüber hinaus gibt es in einigen Branchen besondere gesetzliche Anforderungen, z. B. im Gesundheitsbereich oder in der Finanzwirtschaft (MaRisk – Mindestanforderungen an das Risikomanagement), die in dieser Stellungnahme nicht betrachtet werden.

Mit dem „Three Lines of Defense Model“ (i. F.: 3LoD-Modell) vertritt das Institute of Internal Auditors (IIA) ein Rahmenkonzept, bei dem u. a. die verschiedenen Funktionen des Überwachungssystems bisher konsequent voneinander getrennt dargestellt werden. Dies erfolgt nicht zuletzt wegen der unterschiedlichen Zielsetzungen und der angestrebten Unabhängigkeit der Internen Revision. In der Praxis finden sich aber auch Organisationsansätze, die Teile und Funktionen des Überwachungssystems integrieren oder synergetisch miteinander verknüpfen.

Diese Stellungnahme des gemeinsamen Arbeitskreises „Interne Revision und Risikomanagement“ von DIIR und RMA stellt verschiedene Organisationsformen mit ihren Vor- und Nachteilen dar und zeigt nicht nur die daraus resultierenden Herausforderungen auf, sondern bietet Empfehlungen, damit in der Praxis umzugehen. Es wird zugleich verdeutlicht, dass es nicht nur die eine Organisationsform in der Praxis gibt, sondern verschiedene Varianten des 3LoD-Modells existieren, die unter bestimmten Voraussetzungen auch sinnvoll sein können.

Die Stellungnahme wendet sich an diejenigen, die aufgrund rechtlicher oder sonstiger Anforderungen zur Einrichtung, zum Betreiben und/oder zur Beaufsichtigung eines Überwachungssystems mit seinen Komponenten Risikomanagement- und Revisionssystem verpflichtet sind oder diese freiwillig gestalten 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. 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 von Risikomanagement und Interner Revision

Risikomanagement ist einerseits eine generelle unternehmerische Aufgabe und andererseits eine konkrete Aufforderung an das Unternehmen zur Gestaltung eines Risikomanagementsystems hinsichtlich Aufbau- und Ablauforganisation. Ziel soll es dabei sein, ein unternehmensweites, integriertes und effektives Risikomanagementsystem unter Berücksichtigung der unternehmensspezifischen Gegebenheiten zu gestalten. 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. Diese Aufgabenteilung bedarf einer kritischen Prüfung, die von der Unternehmensleitung und den Aufsichtsgremien sowie externen Prüfern vorgenommen werden kann. 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 Unternehmensmitarbeitende 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.

Andererseits unterstützt die Interne Revision das Risikomanagement bei der Risikoidentifikation und bei der Überprüfung von Risikominderungsmaßnahmen. Es ist darüber hinaus

Aufgabe der Internen Revision, im Ganzen oder im Einzelfall die Wirksamkeit des Risikomanagements zu überprüfen.

Im Unterschied zum Risikomanagement ist die Interne Revision organisatorisch unabhängig auszugestalten. Gemäß den Internationalen Standards bedeutet Unabhängigkeit, dass keine Umstände vorliegen, die die Fähigkeit der Internen Revision beeinträchtigen, ihre Aufgaben unbeeinflusst wahrzunehmen. Dazu sollte die Leitung der Internen Revision direkten und unbeschränkten Zugang zur Geschäftsleitung und ggf. zum Überwachungsorgan haben. Organisatorische Unabhängigkeit ist sichergestellt, wenn die Leitung der Internen Revision funktional an Geschäftsleitung und ggf. an das Überwachungsorgan berichtet. Beispiele für funktionale Unterstellung sind folgende Aktivitäten von Geschäftsleitung bzw. Überwachungsorgan:

- Genehmigung der Geschäftsordnung, des risikoorientierten Revisionsplans und des Budgets und Ressourcenplans für die Interne Revision,
- Annahme von Berichten der Leitung der Internen Revision über die Aufgabenerfüllung der Internen Revision,
- Genehmigen von Entscheidungen bezüglich der Bestellung oder Entlassung der Leitung der Internen Revision sowie ihrer Vergütung.

Wenn die Leitung der Internen Revision Verantwortlichkeiten außerhalb der Internen Revision wahrnehmen soll, muss die Geschäftsleitung Vorkehrungen zur Begrenzung von Beeinträchtigungen der Unabhängigkeit und der Objektivität treffen.

In der Funktion von Risikomanagement und Interner Revision lassen sich vereinfachend folgende Unterschiede benennen: Risikomanagement befasst sich mit zukünftigen Chancen und Gefahren, die Interne Revision überprüft risiko- und zukunftsorientiert getätigte oder bislang unterlassene Maßnahmen hinsichtlich Angemessenheit und Wirksamkeit.

Aus der gegenseitigen Unterstützung, der Einbeziehung der Revision in das Risikomanagementsystem und der Prüfung des Risikomanagements durch die Revision ergeben sich wechselseitige Verbindungen und ein Zusammenwirken im Überwachungssystem, das eine hohe Bedeutung für die Effektivität der Unternehmenssteuerung insgesamt hat.

Im Folgenden sollen die organisatorischen Einheiten (Abteilungen) des Risikomanagements und der Internen Revision im Mittelpunkt der Betrachtung stehen.

2.2 Methodische Gemeinsamkeiten und Unterschiede

Die **Interne Revision** ist Bestandteil des internen Überwachungssystems und hat neben den wesentlichen operativ tätigen Unternehmensbereichen auch die Prozesse der anderen Überwachungsfunktionen (neben dem Risikomanagement z. B. auch Compliance, Controlling oder Qualitätsmanagement) und interne Kontrollen in ihre Prüfungstätigkeiten einzubeziehen („Audit Universe“).

Sie prüft mit Blick auf die Funktionsfähigkeit des Risikomanagementsystems gemäß DIIR Revisionsstandard Nr. 2, dass:

- die Ziele der Organisation mit deren Zweck und Grundausrichtung in Einklang stehen und diese unterstützen,
- 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.

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- und RMA-Arbeitskreis „Interne Revision und Risikomanagement“ entwickelt hat.[1]

Auch das **Risikomanagement** bezieht gemäß der gängigen Risikomanagementstandards ISO 31000 oder COSO ERM alle wesentlichen Funktionen und operativen Bereiche im Unternehmen in den Analyseumfang mit ein („Risk Universe“).

Revision und Risikomanagement sind also gleichermaßen unter Berücksichtigung der Wesentlichkeit aufgefordert, jeweils unternehmensweit zu wirken.

Ein methodischer Unterschied besteht darin, dass im Risikomanagement eine quantifizierte Einschätzung von Risikopotenzialen erfolgt, bei einer Revisionsprüfung die tatsächlichen Schwachstellen bzw. mögliche Optimierungspotenziale im Vordergrund stehen, die in der Praxis häufig qualitativ bewertet werden. Für das Risikomanagement sind eine quantitative Bewertung mit Blick auf Liquidität und Eigenkapital oder EBIT und Verschuldungsgrad sowie

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

eine Aggregation zum Gesamtrisiko unabdingbar, um die Risikotragfähigkeit des Unternehmens zu bestimmen. Diese Gesamtschau der möglichen Risiken eines Unternehmens oder einer Unternehmensgruppe ist in der Regel dem Risikomanagement vorbehalten und erfolgt nicht durch die Revision.

Auch in der konkreten Arbeitsplanung und -durchführung bestehen Unterschiede. Das Risikomanagement, abgesehen von ad-hoc-Meldungen, ist ein zyklischer Prozess, bei dem zumeist mindestens einmal jährlich eine Risikoinventur mit anschließender Risikobewertung vorgenommen wird. Die Interne Revision geht bei ihrer Prüfungstätigkeit von einer risikoorientierten, mindestens jährlichen erstellten Planung aus, die durch ungeplante, aus gegebenem Anlass entstehende Prüfungen ergänzt werden kann. Beide Bereiche 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 Bestimmung 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, Risikokategorien und Risikobewertungssysteme von den Organisationseinheiten in Revision und Risikomanagement verwendet werden. Hierzu sollten sich die Organisationszuständigen abstimmen und im Unternehmen auf geeignete Weise kommunizieren.

Bei der Aufteilung der Prüfungseinheiten und -felder für Zwecke der Revision bzw. in Risikoeinheiten und -felder im Risikomanagement sollten sich die Organisationszuständigen ebenfalls eng abstimmen. Dabei werden beide Bereiche ihre Analyse- und Berichtsebenen differenziert, das heißt in mehreren Dimensionen, wie Geschäftsbereiche, Regionen, Gesellschaften/rechtliche Einheiten, Funktionen oder Projekte, behandeln.

Eine vollständige Deckungsgleichheit wird vermutlich nicht herstellbar sein. Abweichungen zwischen Revision und Risikomanagement können sich z. B. dann ergeben, wenn die Revision Legaleinheiten, beispielsweise Tochtergesellschaften, als Prüfobjekt festlegt und dort bestimmte Funktionsbereiche wie Rechnungswesen, Logistik, Einkauf, Vertrieb, Informationstechnik oder Personalwesen prüfen möchte.

Das Risikomanagement definiert die Risikoeinheiten häufig entsprechend der Management-Reporting-Struktur 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 insbesondere auch im Berichtswesen aus. Beide Funktionen haben in der Regel bereits etablierte

Berichte, sowohl in der Form als auch im Adressatenkreis. Eine Harmonisierung des Berichtswesens wäre zwar im Sinne der Berichtsempfänger wünschenswert, eine getrennte Berichterstattung von Revision und Risikomanagement kann aber 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. Außerdem ist im Sinne einer adressatenorientierten Berichterstattung eine formale und begriffliche Harmonisierung anzustreben.

3.2 Kommunikation und Informationsaustausch

3.2.1 Auskunftsrechte und -pflichten sowie Kommunikationswege

Zwischen Revision und Risikomanagement ist ein direkter, unmittelbarer 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.
- 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.

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

3.2.2 Zeitpunkt und Häufigkeit 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 (Jahres-)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 bestehender Regelungen und Maßnahmen sowie zur frühzeitigen Identifikation neuer wesentlicher Risiken erhalten.

4 Organisationsformen

Bei der Bestimmung der Organisationsformen für Risikomanagement und Revision müssen die im 3LoD-Modell veranschaulichte Reinform der unabhängigen Internen Revision und verschiedene, in der Praxis vorkommende Mischformen berücksichtigt werden.

Das 3LoD-Modell dient als Veranschaulichung eines funktionsfähigen und wirksamen Steuerungs- und Überwachungssystems in Unternehmen, welches insbesondere die Unabhängigkeit der Internen Revision hervorhebt. Es besteht insbesondere aus drei Verteidigungslinien, die u. a. insgesamt eine wirksame Überwachung des Unternehmens bezüglich der Risiken sicherstellen sollen:

1. LoD – Operatives Management als Risiko-Verantwortlicher, zuständig für Risikobehandlung, interne Kontrollen bzw. Internes Kontrollsystem

2. LoD – Ausgestaltung der Managementsysteme und Risikosteuerung

3. LoD – Unabhängige Interne Revision

Der Abschlussprüfer (Wirtschaftsprüfer) und Regulatoren bilden ergänzende externe Verteidigungslinien. Abbildung 1 zeigt die Zuordnung der verschiedenen Funktionsbereiche.

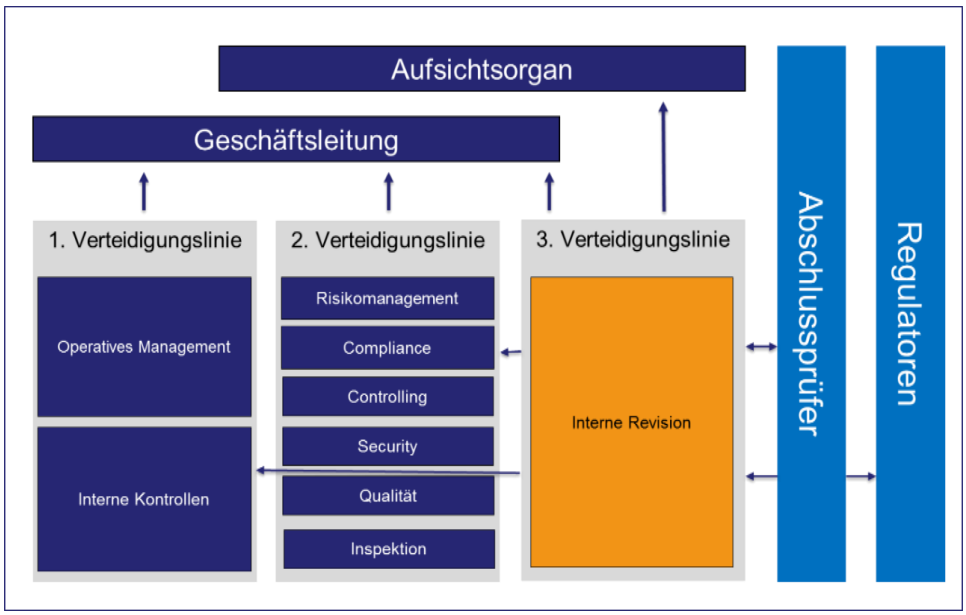

Abb. 1: 3LoD-Modell mit strikter Trennung der Überwachungsaufgaben

Das 3LoD-Modell beinhaltet eine klare Aufgabenunterscheidung der beteiligten Bereiche. Dessen ungeachtet gibt es die Notwendigkeit einer intensiven Zusammenarbeit und Koordination. Das gilt ebenso bei Abänderungen dieses Grundmodells.

4.1 Besonderheiten im 3LoD-Modell

4.1.1 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 erste Verteidigungslinie (sowie die anderen Elemente der zweiten Linie) und die Interne Revision prüft sämtliche Komponenten der ersten und zweiten Verteidigungslinie. 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, unterschiedliche Methoden und Begriffe). 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.

4.1.2 Prüfungsfokus der 3. LoD hängt von der Stärke der Überwachungsfunktion der 2. LoD ab

Das Verständnis der eigenen Überwachungsaufgaben ist nicht nur in verschiedenen Unternehmen, sondern auch innerhalb der Unternehmen in den verschiedenen Bereichen der 2. LoD oft unterschiedlich ausgeprägt. In Abhängigkeit davon gestaltet sich auch die Arbeit der 3. LoD unterschiedlich.

Fokussiert sich die 2. LoD tendenziell auf die Vorgabe von Regelungen oder die Gestaltung von Managementsystemen und weniger auf die Überwachung, ob die Regelungen von der

1. LoD eingehalten werden, dann wird die Revisionsarbeit sich stärker auf die Prüfung der 1. LoD konzentrieren müssen, um eine Aussage zur Funktionsfähigkeit von Systemen oder der tatsächlichen Implementierung von Vorgaben treffen zu können.

Je mehr die 2. LoD Überwachungsaufgaben ausübt, um sich selbst von der Einhaltung von Regeln zu überzeugen, desto stärker können sich die Revisionsaufgaben auf die Prüfung der 2. LoD ausrichten, insbesondere wie diese die Funktionsfähigkeit und Regeleinhaltung sicherstellt. Die Modellausprägung mit einer eher überwachenden Risikomanagementfunktion stärkt insgesamt die Sicherheit im Unternehmen, erfordert im Gegenzug jedoch entsprechende Kompetenzen und Ressourcen in der 2. LoD. Diese Ressourcen können entweder aufgebaut oder mit externer Unterstützung bereitgestellt werden. Es hängt von den Erwartungen der Unternehmensführung an die Ausgestaltung des Risikomanagementsystems ab, inwieweit die 2. LoD nur gestalterisch oder auch überwachend tätig wird.

Ferner wird der Prüfungsfokus der Revision als 3. LoD nicht unerheblich vom Reifegrad des Risikomanagements in der 2. LoD bestimmt. Ist das Risikomanagement, wie noch in vielen – vor allem kleineren oder jungen – Unternehmen der Fall, noch nicht sehr stark entwickelt bzw. gar nicht vorgesehen, so muss sich der Prüfungsfokus der Revision dahin verschieben, dass sie zunächst selbst die wesentlichen Risiken identifiziert. Ein zentrales Prüfungsergebnis kann die Empfehlung zur Einführung von adäquaten Risikomanagementprozessen sein. Erst ein ausgereiftes und vollständig implementiertes Überwachungssystem im Sinne des 3LoD-Modells stellt sicher, dass Risiken systematisch gesteuert werden und die unternehmensinterne Risikokommunikation gewährleistet wird. Bei einer voll ausgereiften 2. LoD steht dann folgerichtig für die Revision eher die Prüfung der Wirksamkeit des Risikomanagementsystems sowie der Kommunikationswege im Vordergrund.

Das IIA hat in einem Positionspapier im Januar 2013 die Bedeutung des 3LoD-Modells für das Risikomanagement hervorgehoben:

> *„Risk management normally is strongest when there are three separate and clearly identified lines of defense."*

Wie geschildert, können Strategie und Prüfungsfokus der Revision aber auch im 3LoD-Modell nicht pauschal definiert werden, sondern müssen an die jeweiligen Erwartungen und Reifegrade in den Unternehmen angepasst werden.

4.2 Besonderheiten in Mischformen

4.2.1 Vor- und Nachteile einer Kombinationsform von Risikomanagement und Revision

Die besonderen 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 Abschnitt 3 aufgeführten Anforderungen an die Zusammenarbeit von Risikomanagement und 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 Revision, denn in den Gebieten, in denen die Revision selbst operative Aufgaben übernimmt, kann sie keine unabhängige Prüfung der Wirksamkeit 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 weitere 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 3LoD-Modell der 2. LoD (Systemgestaltung und Risikomanagementprozesse) zuzuordnen sind. Eine eigenständige Risikomanagementfunktion existiert in diesem Fall in der 2. LoD 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 insbesondere die operative Identifizierung, Bewertung und das organisa-

torische Management der Risiken 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 der Geschäftsleitung durchgeführt werden.

Teilintegration – die Revision übernimmt Aufgaben der Systemgestaltung ohne diesbezügliche Wirksamkeitsprüfung

Im Gegensatz zur Vollintegration übernimmt die Revision bei der Teilintegration ebenfalls Aufgaben der 2. LoD, aber nur in der Systemgestaltung. Diese systemischen Vorgaben werden dann – getrennt von der Revision - durch die operativen Einheiten der ersten Verteidigungslinie 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 3LoD-Aufgabe unabhängig wahrgenommen werden, da sie anders als bei der Vollintegration daran nicht unmittelbar beteiligt ist. Die Gestaltung des Risikomanagementsystems kann sie nicht unabhängig prüfen.

4.2.3 Weitere Mischmodelle zur Überwachung des Unternehmens

Die vorliegende Ausarbeitung 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. Hierbei werden häufig Aufgaben des Risikomanagements oder des Compliance Systems in die Interne Revision integriert. Faktisch haben sich in der Unternehmenswelt diverse Kombinationen etabliert, da durch auf die jeweilige Situation zugeschnittene Organisationsformen Effizienz- und Effektivitätsvorteile erwartet werden.

Darüber hinaus kommen in der Praxis weitere Kombinationsformen vor, bei denen auch technische Funktionen (z. B. Qualitätsmanagement) oder spezielle Überwachungsfunktionen (z. B. Geldwäschebeauftragte, Ombudsleute oder Umweltbeauftragte) eine bedeutsame Rolle im Risikomanagement spielen.

4.2.4 Interessenskonflikte 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 dann die Objektivität der Prüfung. In diesen Fällen ginge also die Verantwortung der Revision über die 3. LoD hinaus. 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 (Standard 1112). Z. B. wird eine zeitliche Begrenzung der zusätzlichen Aufgaben oder das Entwickeln alternativer (unabhängiger) Prüfungsprozesse vorgeschlagen.

Aus Sicht der Geschäftsleitung ergeben sich in Mischformen immer Einschränkungen für die Unabhängigkeit der Internen Revision. In den Gebieten und Fällen, in denen die Revision selbst operative Aufgaben übernimmt, kann sie nicht zugleich eine unabhängige Prüfung und Bewertung in diesen Bereichen vornehmen. In der Praxis ergeben sich dennoch unterschiedliche Konstellationen. Diese unterscheiden sich in ihrer Ausprägung je nach Integrationsgrad, Organisationsform oder Führungsmodell. Entsprechend wären im Rahmen von Mischformen neben deren Vor- und Nachteilen stets auch die Maßnahmen zur Verringerung von Interessenkonflikten zu diskutieren:

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

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

- Gemeinsame Darstellung der Tätigkeiten von Revision und Risikomanagement 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 durch das operativ tätige Management selbst erlauben.

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 der 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 3LoD-Modells 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 z. B. durch die Einschaltung externer, unabhängiger Prüfungsdienstleister möglicherweise 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 Verteidigungslinie neben Effizienzvorteilen bei der Systemgestaltung und -überwachung 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 aber 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) und Jörg Uffelmann.

In der Version 1.0 veröffentlicht am 11.05.2020 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