Stellungnahme der RMA Risk Management & Rating Association e.V. zur neuen Fassung des Deutschen Corporate Governance Kodex vom 05.08.2026

1. Anlass und Ziel dieser Stellungnahme

Die Regierungskommission Deutscher Corporate Governance Kodex hat am 5. August 2026 Vorschläge zur Änderung des Deutschen Corporate Governance Kodex (DCGK) veröffentlicht und zur Konsultation gestellt. Die angestrebte Weiterentwicklung und insbesondere die Vereinfachung des Kodex sind grundsätzlich zu begrüßen. Dies gilt insbesondere dort, wo bestehende Empfehlungen lediglich gesetzliche Anforderungen wiederholen oder keinen erkennbaren zusätzlichen Beitrag zu einer guten Unternehmensführung leisten.

Die Vereinfachung des Kodex sollte jedoch zugleich zum Anlass genommen werden, bestehende inhaltliche Lücken zu schließen. Aus Sicht der RMA betrifft dies insbesondere den Umgang mit Chancen und Risiken sowie deren Berücksichtigung bei unternehmerischen Entscheidungen. Gerade vor dem Hintergrund eines zunehmend von geopolitischen Veränderungen, technologischen Umbrüchen und wirtschaftlichen Unsicherheiten geprägten Unternehmensumfelds kommt einem leistungsfähigen Risikomanagement eine besondere Bedeutung zu.

Hinzu kommt, dass sich die gesetzlichen Anforderungen an das Risikomanagement und Krisenfrüherkennung in den vergangenen Jahren weiterentwickelt haben. Insbesondere die mit § 1 StaRUG verbundenen Anforderungen an die Früherkennung möglicher bestandsgefährdender Entwicklungen finden im DCGK bisher nur unzureichend Berücksichtigung. Der vorliegende Konsultationsentwurf ändert daran aus Sicht der RMA nichts Wesentliches. Grundsatz 4 beschränkt sich weiterhin auf die allgemeine Forderung nach einem angemessenen und wirksamen internen Kontroll- und Risikomanagementsystem.

Auch nachhaltigkeitsbezogene Risiken und Chancen sollten nicht losgelöst vom unternehmerischen Risikomanagement betrachtet werden. Soweit sie eine kritische Schwelle überschreiten, sollten sie gemeinsam mit strategischen, finanziellen, operativen und sonstigen Risiken und Chancen in die bestehenden Risikomanagement- und Unternehmenssteuerungsprozesse integriert werden. Eine solche integrierte Betrachtung vermeidet parallele Strukturen und trägt dazu bei, Nachhaltigkeitsaspekte dort zu berücksichtigen, wo sie für unternehmerische Entscheidungen und die Risikoposition des Unternehmens relevant sind.

Darüber hinaus müssen aus Sicht der RMA auch die Informationswege zum Aufsichtsrat gestärkt werden. Die direkte Kommunikation zwischen Risikomanagement, Interner

Revision und Aufsichtsrat sollte für alle vom Kodex erfassten Unternehmen verbindlich vorgesehen werden.

Die RMA möchte mit dieser Stellungnahme daher einige konkrete Vorschläge unterbreiten, wie die Themen Risikomanagement, Krisenfrüherkennung, unternehmerische Entscheidungen und Überwachung durch den Aufsichtsrat im DCGK stärker miteinander verknüpft und die bestehenden gesetzlichen Anforderungen angemessen berücksichtigt werden können.

2. Risikoorientierte unternehmerische Entscheidungen

Unternehmerische Entscheidungen zu treffen, gehört zu den zentralen Aufgaben der Geschäftsführung und damit zu den Kernelementen guter Corporate Governance. Ihre Wirkungen entfalten Entscheidungen jedoch in der Zukunft, deren Entwicklung zum Entscheidungszeitpunkt nicht mit Sicherheit bekannt sein kann. Der Umgang mit dieser Unsicherheit ist eine zentrale Aufgabe des Risikomanagements.

Risikomanagement soll die Qualität unternehmerischer Entscheidungen verbessern, indem Unsicherheit verstanden und ggf. reduziert wird. Zudem werden so risikorelevante Informationen aggregiert, und eine kritische Reflexion im Entscheidungsprozess wird gefördert.[1] Voraussetzung hierfür ist, dass Risikomanagement als Grundlage unternehmerischer Entscheidungen verstanden und die damit verbundenen Chancen und Risiken bei deren Vorbereitung und Bewertung systematisch berücksichtigt werden.[2]

Dieser Gedanke steht in engem Zusammenhang mit der Business Judgement Rule nach § 93 Abs. 1 Satz 2 AktG, welche fordert, dass unternehmerische Entscheidungen auf Grundlage angemessener Informationen zu treffen sind. Dazu gehört insbesondere, die zur Verfügung stehenden Handlungsalternativen im Hinblick auf ihre jeweiligen Chancen und Risiken zu analysieren und auf dieser Grundlage unter Anwendung geeigneter betriebswirtschaftlicher Methoden gegeneinander abzuwägen.

Aus Sicht der RMA sollte im DCGK deutlicher herausgestellt werden, dass bei wesentlichen unternehmerischen Entscheidungen nachvollziehbar dargestellt werden muss, welche wesentlichen Chancen und Risiken mit den betrachteten Handlungsalternativen verbunden sind und wie sich die Entscheidung auf die Risikoposition des Unternehmens auswirkt. Gerade bei Entscheidungen, die den Risikoumfang wesentlich erhöhen können, sollte zudem geprüft werden, ob die Risikotragfähigkeit des Unternehmens weiterhin gewährleistet ist. Wir schlagen daher vor, eine zusätzliche Empfehlung vor der

[1] Vgl. Hunziker, S./Giesen, K. (2025): Entscheidungsorientiertes Risikomanagement – Wie Risikomanagement zum strategischen Entscheidungspartner wird, ZRFC – Risk, Fraud & Compliance, 20. Jg., Heft 5/2025, S. 206–211.
[2] Vgl. Giesen, K./Gleißner, W. (2025): Unternehmensentscheidungen in unsicheren Zeiten, in: Christ, J. P./Giesen, K. (Hrsg.): Polykrisen, Strukturbrüche und Schwarze Schwäne – Unternehmerische Entscheidungsfindung und Wirtschaftspolitik unter veränderten Rahmenbedingungen der 2020er-Jahre, Springer Gabler, Wiesbaden, S. 17–40.

derzeitigen Empfehlung A.1 (als neue A.1 mit entsprechender Neu-Nummerierung der folgenden Empfehlungen) einzufügen, die dem Rechnung trägt.

Formulierungsvorschlag für neue Empfehlung vor bisher A.1:
„Der Vorstand soll bei wesentlichen unternehmerischen Entscheidungen nachvollziehbar darstellen, welche wesentlichen Chancen und Risiken mit den betrachteten Handlungsalternativen verbunden sind und wie sich die Entscheidung auf die Risikoposition der Gesellschaft bzw. des Unternehmens auswirkt. Bei Entscheidungen, die den Gesamtrisikoumfang wesentlich erhöhen können, soll zudem geprüft werden, ob die Risikotragfähigkeit des Unternehmens weiterhin gewährleistet ist.“

3. Vorausschauendes Risikomanagement und Aggregation von Risiken

Die heutige Risikolandschaft von Unternehmen ist zunehmend durch Interdependenzen, hohe Veränderungsgeschwindigkeit und nichtlineare Entwicklungen geprägt. Eine überwiegend auf die Identifikation, Bewertung und Fortschreibung einzelner Risiken ausgerichtete Betrachtung greift insbesondere unter diesen Bedingungen zu kurz.

Für die Wirksamkeit des Risikomanagements gewinnen deshalb insbesondere Frühwarnfähigkeit, Szenario-Analysen und die Berücksichtigung von Wechselwirkungen zwischen Risiken im Rahmen einer Aggregation der Risiken auf Gesellschafts- bzw. Unternehmensebene an Bedeutung. Empirische Untersuchungen zeigen, dass Rollen und Eskalationswege des Risikomanagementsystems vielfach definiert sind, dass aber häufig belastbare Frühwarnsysteme, szenario-basierte Analysen und Risikoaggregationen fehlen oder unzulänglich ausgestaltet sind. Risikomanagement bleibt dadurch tendenziell reaktiv und kann nicht wirksam zur Überwachung der Risikotragfähigkeit von Gesellschaften bzw. Unternehmen beitragen.

Der Kodex sollte bewusst keine bestimmten Methoden oder Instrumente vorschreiben. Ziel sollte vielmehr sein, die vorausschauende Steuerungsfähigkeit auf Ebene der Gesamtrisiken von Gesellschaften bzw. Unternehmen als Merkmal eines wirksamen Risikomanagements zu verankern. Entsprechend sollte Grundsatz 4 ergänzt werden.

Formulierungsvorschlag für Grundsatz 4:
„Für einen verantwortungsvollen Umgang mit den Risiken der Geschäftstätigkeit bedarf es eines angemessenen und wirksamen internen Kontrollsystems und Risikomanagementsystems. Das Risikomanagementsystem ist angemessen und wirksam ausgestaltet, wenn es einerseits Risiken auf Gesellschafts- bzw. Unternehmensebene aggregiert und somit Risikointerdependenzen berücksichtigt sowie andererseits durch Frühwarnindikatoren oder ähnliche Kennziffern vorausschauend ausgestaltet ist. Die Angemessenheit und Wirksamkeit des internen Kontrollsystems und Risikomanagementsystems setzen deren interne Überwachung voraus.“

4. Risikomanagement und Krisenfrüherkennung

Mit § 1 StaRUG hat der Gesetzgeber die Anforderungen an die Krisenfrüherkennung konkretisiert. Die Geschäftsleiter haftungsbeschränkter Unternehmen sind verpflichtet, fortlaufend über Entwicklungen zu wachen, welche den Fortbestand des Unternehmens gefährden können. Werden entsprechende Entwicklungen erkannt, sind geeignete Gegenmaßnahmen zu ergreifen und die Überwachungsorgane unverzüglich zu informieren.

Aus logischen Erwägungen ist zu beachten, dass jedes Unternehmen potenziell im Bestand gefährdet ist. Entscheidend ist daher nicht die grundsätzliche Möglichkeit einer Bestandsgefährdung, sondern das Ausmaß der Bestandsgefährdung resultierend aus den bestehenden Risiken. Im Fokus sollte folglich die Frage stehen, wie ausgeprägt die Bestandsgefährdung ist und ob die Risikosituation bereits ein kritisches Niveau erreicht.

Für eine fundierte Beurteilung dieser Bestandsgefährdungen ist daher eine Identifikation, Quantifizierung und insbesondere Aggregation der wesentlichen Risiken erforderlich, um diesen Grad der Bestandsgefährdung zu schätzen. Genau diese Verbindung zwischen Risikoaggregation, Bestandsgefährdung und Krisenfrüherkennung wurde bereits in den bisherigen Vorschlägen zur Weiterentwicklung des DCGK herausgestellt.[3] [4] [5]

Der aktuelle Konsultationsentwurf greift diese Entwicklung aus Sicht der RMA weiterhin nicht ausreichend auf. Grundsatz 4 stellt zwar zutreffend fest, dass ein verantwortungsvoller Umgang mit den Risiken der Geschäftstätigkeit ein angemessenes und wirksames internes Kontrollsystem und Risikomanagementsystem erfordert. Eine Konkretisierung hinsichtlich der Identifikation, Quantifizierung und Aggregation von Risiken sowie der Beurteilung möglicher bestandsgefährdender Entwicklungen erfolgt jedoch nicht.

Dies erscheint insbesondere deshalb problematisch, weil die Betrachtung einzelner Risiken keine verlässliche Aussage über den Grad der Bestandsgefährdung eines Unternehmens erlaubt. Risiken können sich gegenseitig verstärken, gleichzeitig eintreten oder über gemeinsame Ursachen miteinander verbunden sein. Umgekehrt können sich Risiken teilweise auch kompensieren. Erst die Aggregation der Risiken mit Bezug auf die Unternehmensplanung ermöglicht daher eine fundierte Beurteilung, ob die Risikotragfähigkeit eines Unternehmens gefährdet ist und gegebenenfalls Maßnahmen der Krisenprävention erforderlich werden.

Aus Sicht der RMA sollte der DCGK diese Anforderungen ausdrücklich aufgreifen. Zu Grundsatz 4 sollte daher eine zusätzliche Empfehlung vor der derzeitigen Empfehlung

---

[3] Bantleon, U. et al. (2025): Risikomanagement, Business Judgement Rule, Nachhaltigkeit: Neue Anforderungen für den Deutschen Corporate Governance Kodex (DCGK) (Teil I) – Stellungnahme und Verbesserungsvorschläge, DER BETRIEB, 78. Jg., Heft 34, S. 2043–2049.

[4] Bantleon, U. et al. (2025): Risikomanagement, Business Judgement Rule, Nachhaltigkeit: Neue Anforderungen für den Deutschen Corporate Governance Kodex (DCGK) (Teil II) – Stellungnahme und Verbesserungsvorschläge, DER BETRIEB, 78. Jg., Heft 35, S. 2111–2119.

[5] Bantleon, U. et al. (2025): Weiterentwicklung des Deutschen Corporate Governance Kodex (DCGK) – Ein Appell, ZRFC – Risk, Fraud & Compliance, 20. Jg., Heft 5/2025, S. 199–201.

A.3 (mit entsprechender Neu-Nummerierung der folgenden Empfehlungen) eingefügt werden. Diese neue Empfehlung sollte den Gedanken der Krisenfrüherkennung aufgreifen und die Risikoaggregation als wesentlichen Bestandteil eines angemessenen Risikomanagementsystems verankern.

Formulierungsvorschlag für neue Empfehlung vor bisher A.3:
„Das Risikomanagementsystem soll eine systematische Identifikation, eine sachgerechte Quantifizierung und Aggregation der Risiken in Bezug auf die Unternehmensplanung beinhalten, um den Grad der Bestandsgefährdung des Unternehmens zu bewerten. Bei Überschreiten eines kritischen Schwellenwerts der Bestandsgefährdung sollen Maßnahmen der Krisenprävention eingeleitet werden.“

5. Integrierte Betrachtung aller Risiken und Chancen

Nachhaltigkeitsbezogene Risiken sollten nicht als separate Risikokategorie außerhalb des unternehmerischen Risikomanagements behandelt werden. Sie können erhebliche finanzielle, operative und strategische Auswirkungen entfalten und sollten daher – soweit wesentlich – in die bestehenden Steuerungs- und Risikomanagementprozesse integriert werden.

Die Praxis zeigt hier weiterhin eine erhebliche Integrationslücke. Nachhaltigkeit ist in vielen Unternehmen formal etabliert, die methodische Anschlussfähigkeit an das Risikomanagement ist jedoch häufig noch nicht ausreichend gegeben. Dies begünstigt parallele, compliance-orientierte Strukturen, anstatt Nachhaltigkeitsrisiken und -chancen in die reguläre Unternehmenssteuerung einzubeziehen.

Eine entsprechende Ergänzung der Empfehlung A.3[6] aus der neuen Fassung des DCGK sollte daher nicht implizieren, dass separate ESG-Governance-Strukturen etabliert werden. Im Gegenteil: Sie sollte dazu beitragen, Nachhaltigkeit aus separaten Strukturen herauszulösen und dort zu integrieren, wo wesentliche Risiken und Chancen hingehören – im unternehmerischen Risikomanagement und in der Unternehmenssteuerung.

Formulierungsvorschlag für Empfehlung A.3 alt:
„Das interne Kontrollsystem und Risikomanagementsystem sollen, soweit nicht bereits gesetzlich geboten, auch nachhaltigkeitsbezogene Ziele, Risiken und Chancen abdecken. Wesentliche strategische, finanzielle, operative, nachhaltigkeitsbezogene und sonstige Risiken und Chancen sollen integriert betrachtet und angemessen in die Unternehmenssteuerungs-, Risiko-, Kontroll- und Compliance-Prozesse einbezogen werden. Dies soll die Prozesse und Systeme zur Erfassung und Verarbeitung der hierfür erforderlichen Daten einschließen.“

[6] Nach Einfügung zusätzlicher Empfehlungen vor der A.1 und A.3 aus der Neufassung des DCGK (siehe Punkte 2. und 4. dieses Dokuments) würde diese Empfehlung hier als A.5 zu nummerieren sein.

6. Informationsversorgung des Aufsichtsrats

Ein leistungsfähiges Risikomanagement kann vor allem dann einen wirksamen Beitrag zur Corporate Governance leisten, wenn die Risiko-Informationen auch den Aufsichtsrat erreichen. Der Aufsichtsrat muss in die Lage versetzt werden, die Risikosituation des Unternehmens sowie die Angemessenheit und Wirksamkeit des Risikomanagementsystems eigenständig beurteilen zu können.

Der DCGK trägt diesem Gedanken grundsätzlich Rechnung. Nach Grundsatz 16 informiert der Vorstand den Aufsichtsrat regelmäßig, zeitnah und umfassend unter anderem über die Risikolage und das Risikomanagement. Damit erfolgt die Informationsversorgung des Aufsichtsrats jedoch im Wesentlichen durch das Organ, das dieser überwachen soll.

Aus Sicht der wohlbekannten Principal-Agent-Theorie entsteht hieraus ein grundlegendes Governance-Problem: Zwischen Vorstand und Aufsichtsrat besteht eine Informationsasymmetrie, da der Vorstand als Agent regelmäßig über einen erheblichen Informationsvorsprung gegenüber dem Aufsichtsrat als Principal verfügt. Eine wirksame Überwachung setzt daher voraus, dass der Aufsichtsrat die vom Vorstand bereitgestellten Informationen kritisch würdigen und bei Bedarf durch unabhängige Informationsquellen ergänzen kann.

Mit dem FISG wurde dieser Gedanke bereits aufgegriffen. § 107 Abs. 3 AktG stärkt die unmittelbare Kommunikation des Prüfungsausschusses mit den Leitern derjenigen Zentralbereiche, die seine Aufgaben betreffen. Angesichts der zentralen Bedeutung des Risikomanagements, der Internen Revision und des internen Kontrollsystems sollte eine entsprechende direkte Kommunikation mit dem Aufsichtsrat beziehungsweise Prüfungsausschuss im DCGK für alle Unternehmen verbindlich vorgesehen werden.

Dies schränkt die Verantwortung des Vorstands für die Information des Aufsichtsrats nicht ein. Vielmehr wird die Informationsversorgung um einen zusätzlichen, unabhängigen Informationskanal ergänzt. Der unmittelbare Austausch ermöglicht es dem Aufsichtsrat, die Risikolage und die Funktionsfähigkeit der hierfür relevanten Systeme aus unterschiedlichen Perspektiven zu beurteilen und seiner Überwachungsfunktion besser nachzukommen.

Aus Sicht der RMA sollte der DCGK daher eine direkte Kommunikation zwischen Risikomanagement, Interner Revision und Internem Kontrollsystem einerseits sowie dem Aufsichtsrat beziehungsweise Prüfungsausschuss andererseits verbindlich vorsehen.

Formulierungsvorschlag für Grundsatz 16:
„Die Information des Aufsichtsrats ist Aufgabe des Vorstands. Der Aufsichtsrat hat jedoch seinerseits sicherzustellen, dass er angemessen informiert wird. Zu diesem Zweck soll der Aufsichtsrat bei dem Leiter des Risikomanagements oder einer anderen Funktion, die mit Risikomanagement-Aufgaben betraut ist, direkt Auskünfte einholen können, ohne den Vorstand einzuschalten. Der Vorstand informiert den Aufsichtsrat regelmäßig,

zeitnah und umfassend über alle für das Unternehmen relevanten Fragen insbesondere der Strategie, der Planung, der Geschäftsentwicklung, der Risikolage, des Risikomanagements und der Compliance. Er geht auf Abweichungen des Geschäftsverlaufs von den aufgestellten Plänen und vereinbarten Zielen unter Angabe von Gründen ein. Der Aufsichtsrat kann jederzeit zusätzliche Informationen vom Vorstand verlangen.“

7. Fazit

Die Überarbeitung des Deutschen Corporate Governance Kodex bietet die Chance, diesen nicht nur zu vereinfachen, sondern zugleich an wesentliche gesetzliche und betriebswirtschaftliche Entwicklungen der vergangenen Jahre anzupassen. Gerade im Bereich des Risikomanagements besteht aus Sicht der RMA weiterhin Handlungsbedarf.

Aus Sicht der RMA sollten insbesondere folgende Punkte in der weiteren Überarbeitung des DCGK berücksichtigt werden:

1. Risikomanagement und Krisenfrüherkennung: Der DCGK sollte die Anforderungen an die Früherkennung möglicher bestandsgefährdender Entwicklungen ausdrücklich aufgreifen. Hierzu gehört insbesondere die systematische Identifikation, Quantifizierung und Aggregation wesentlicher Risiken mit Bezug auf die Unternehmensplanung.
2. Risikoorientierte unternehmerische Entscheidungen: Bei wesentlichen unternehmerischen Entscheidungen sollten Chancen und Risiken sowie die Auswirkungen der Entscheidung auf den Risikoumfang des Unternehmens angemessen berücksichtigt werden. Risikomanagement sollte damit nicht erst nach einer Entscheidung ansetzen, sondern bereits Bestandteil ihrer Vorbereitung sein.
3. Integrierte Betrachtung von Risiken und Chancen: Nachhaltigkeitsbezogene Risiken und Chancen sollten nicht isoliert betrachtet werden. Soweit sie wesentlich sind, sollten sie gemeinsam mit strategischen, finanziellen, operativen und sonstigen Risiken und Chancen in die bestehenden Risikomanagement- und Unternehmenssteuerungsprozesse integriert werden.
4. Direkte Kommunikation mit dem Aufsichtsrat: Ergänzend zur Informationspflicht des Vorstands sollte eine direkte Kommunikation zwischen Risikomanagement, Interner Revision und dem Aufsichtsrat beziehungsweise Prüfungsausschuss vorgesehen werden. Dies ermöglicht dem Aufsichtsrat eine zusätzliche, vom Vorstand unabhängige Einschätzung der Risikolage und der Funktionsfähigkeit des Risikomanagementsystems.

Diese Ergänzungen – oben werden entsprechende Formulierungen vorgeschlagen – würden dazu beitragen, das Risikomanagement stärker mit der Unternehmenssteuerung, unternehmerischen Entscheidungen und der Überwachung durch den Aufsichtsrat zu verbinden. Eine solche Weiterentwicklung erscheint gerade in einem von zunehmender Unsicherheit und sich überlagernden Risiken geprägten Unternehmensumfeld als wichtiger Bestandteil guter Corporate Governance.

2. September 2026 **RMA Risk Management & Rating Association e.V.**

Mitwirkende bei der Erstellung der Stellungnahme:

- Prof. Dr. Kristian Giesen, Mitglied des Vorstands der RMA
- Harald Nikutta, Mitglied des Beirats der RMA
- Jan Offerhaus, Mitglied des Vorstands der RMA
- Marco Wolfrum, Stv. Vorsitzender des Vorstands der RMA

Ansprechpartner für Rückfragen:

Jan Offerhaus
RMA Risk Management & Rating Association e.V.
Zeppelinstr. 73
81669 München
E-Mail: jan.offerhaus@rma-ev.org