Risikokultur – im Fokus der Aufsicht

Überblick und Stand der Entwicklung

Als Ursachen für die globale Finanzmarktkrise im Jahr 2008[1] sind Defizite in der Unternehmensführung (Governance) sowie mangelhafte kulturelle Grundlagen im Umgang mit Risiken und ein darauf aufbauendes Versagen in den Instituten zu nennen. Um dem entgegenzuwirken, hatte die Aufsicht im Rahmen ihrer Aufgaben zur Gewährleistung eines sicheren und effektiven Finanzsystems nicht nur den Grundstein zur Schaffung der MaRisk-Compliance-Funktion im Jahr 2012[2] gelegt, sondern mit der CRD IV im Jahr 2013 erstmals eine Erwartungshaltung formuliert, wonach eine solide Risikokultur als Teil des Risikomanagements auf allen Unternehmensebenen zu fördern ist.[3]

2017 hat die BaFin mit der fünften MaRisk-Novelle dann zunächst die Entwicklung, Förderung und Integration einer angemessenen Risikokultur als Aufgabe der Geschäftsleitung im Rahmen ihrer Gesamtverantwortung für eine ordnungsgemäße Geschäftsorganisation in die MaRisk aufgenommen.[4]

Als „Risikokultur" werden hierbei die Normen, Einstellungen und Verhaltensweisen eines Institutes auf das Risikobewusstsein, die Risikobereitschaft und das Risikomanagement sowie Kontrollen definiert, die für Entscheidungen über Risiken maßgeblich sind.[5]

Mit der sechsten MaRisk-Novelle im Jahr 2021 hat die BaFin kleine Änderungen und Klarstellungen im Hinblick auf die Risikokultur eingefügt, wobei diese maßgeblich die Berücksichtigung von ESG-Risiken sowie die Forderung nach einer Überwachung (und Dokumentation) der Risikokultur betreffen. 2023 wurde schließlich mit der siebten MaRisk-Novelle das Thema Überwachung der Risikokultur auf allen Ebenen des Instituts in die MaRisk aufgenommen.

Im Rahmen des Nationalen Aufsichtsprogramms 2025–2027 haben die Bundesbank und die BaFin das Thema Governance, das auch die Aspekte der Risikokultur beinhaltet, als einen zentralen Schwerpunkt der nationalen Bankenaufsicht definiert.[6]

Insgesamt wird Governance damit als Schlüsselfaktor für eine effektive und zukunftsfähige Bankenaufsicht gesehen. Eine solide Governance trägt wesentlich dazu bei, Risiken frühzeitig zu erkennen, Fehlsteuerungen zu vermeiden und Vertrauen in das Bankensystem zu stärken.

Ziele und Elemente einer angemessenen Risikokultur

Allgemein beschreibt die Risikokultur die Art und Weise, wie Mitarbeitende eines Instituts im Rahmen ihrer Tätigkeiten mit Risiken umgehen sollen. Die Identifizierung von und der bewusste Umgang mit Risiken soll durch eine nachhaltige Risikokultur gefördert werden.

Stichpunktartig lassen sich die Ziele der Risikokultur folgendermaßen beschreiben:

- Auseinandersetzung mit den Risiken des operativen Geschäfts (finanzielle/nichtfinanzielle Risiken)
- Schaffung und Förderung eines Risikobewusstseins, welches das tägliche Denken und Handeln prägt
- Entscheidungsprozesse führen zu Ergebnissen, die unter Risikogesichtspunkten ausgewogen sind
- Schaffen von nachhaltigen Geschäftsmodellen

- Etablieren von institutsspezifischen Werten wie Vertrauen, Professionalität und Kundennähe
- Schaffung eines Verantwortungsbewusstseins der Mitarbeitenden im Hinblick auf das Eingehen von Risiken
- Sensibilisierung für Mängel, die dann durch ergebnisorientierte und frühzeitige Maßnahmen zu beheben sind

Die Risikokultur steht nicht isoliert da und ist auch kein neuer Risikomanagementansatz, sondern ist eines von meheren Risikomanagement-Elemente, zusammen mit Interner Governance und Risikomanagement:

Risikokultur	Risikomanagement	Interne Governance
Führung	**Identifikation**	**Strategie**
Verantwortlichkeiten	**Analyse/Quantifizierung**	**Funktionstrennung**
Kommunikation	**Bewertung**	**Kompetenzsystem**
Anreize	**Bewältigung/Steuerung**	**IKS**
	Überwachung & Reporting	**Richtlinien/SfO**
		Berichtswesen

Bei der Frage, ob die Risikokultur eines Hauses angemessen ist, orientiert sich die Aufsicht an den folgenden vier Indikatoren[7], wobei diese weder als abschließend noch als Checkliste zu verstehen sind.[8]

Indikatoren für eine angemessene Risikokultur:[9]

1. Leitungskultur: „Vorleben" der gewünschten Risikokultur und Bekenntnis zu risikoangemessenem Verhalten durch Vorstand und Führungskräfte
2. Verantwortlichkeiten der Mitarbeiterinnen und Mitarbeiter: Tätigkeiten ausrichten am Wertesystem, am festgelegten Risikoappetit und an den bestehenden Risikolimits
3. Offene Kommunikation und kritischer Dialog:
   a. Konstruktive Anregungen und Kritik, alternative Standpunkte offen kommunizieren
   b. Mitarbeitenden ermöglichen, vertrauliche Bedenken über Vorgehensweisen im Institut zu äußern
4. Angemessene Anreizstrukturen schaffen: unterstützende Motivation durch materielle und immaterielle Anreize, sich entsprechend dem Wertesystem zu verhalten und innerhalb der festgelegten Risikolimits und Risikotoleranzen zu agieren

Die Indikatoren der Risikokultur werden durch konkrete, nachhaltige Maßnahmen sichtbar, greifbar und nachprüfbar.

Maßnahmen zur Etablierung und Stärkung der Risikokultur

Seitens der Aufsicht gibt es keine „definierte“ oder „vorgeschriebene“ Risikokultur. Risikokultur ist individuell und abhängig von dem Geschäftsmodell, den Produkten und Kunden, der Eigentümerstruktur und/oder einer Verbundzugehörigkeit sowie dem Proportionalitätsprinzip. Die Risikokultur einer regional tätigen Volksbank Raiffeisenbank sieht anders aus als die einer international agierenden Großbank.

Mit der fünften MaRisk-Novelle[10] hat die Aufsicht die Verantwortlichkeit für das Thema Risikokultur beim Vorstand angesiedelt: Die Mitglieder des Vorstands haben die wichtigste Vorbildfunktion (Tone from the Top); ihre Äußerungen und ihr Verhalten sollen ein Wertesystem widerspiegeln, das die Grundlage für die Risikokultur im Institut darstellt.

Der Vorstand sollte

- fortlaufend verdeutlichen, dass von den Mitarbeitenden ein ethisch und ökonomisch einwandfreies Verhalten erwartet wird, das durch
  - die Einhaltung der festgelegten Risikotoleranzen und der gesetzlichen Vorgaben sowie
  - die gesellschaftliche Erwartungshaltung an Banken geprägt ist;
- das Thema Risikokultur in einer Geschäfts- und Risikostrategie implementieren;
- für eine angemessene Unternehmensstruktur als Teil der Governance sorgen,
  - die sich an den Strategien des Unternehmens ausrichtet und
  - die Transparenz über die Geschäftsaktivitäten und Risiken des Instituts sicherstellt;
- institutsspezifische Werte entwickeln und kommunizieren, die auf den langfristigen und nachhaltigen Geschäftserfolg ausgerichtet sind, wie: Vertrauen – Professionalität – Nachhaltigkeit – Qualität – Regionalität – Kundennähe – Mitgliederverpflichtung;
- Kommunikation, offenen Dialog und Vertrauen auf allen Ebenen fördern („eine Bank – ein Team“):
  - im Aufsichtsrat, im Vorstandsteam, im Führungskreis und unter den Mitarbeitenden,
  - zwischen Vorstand und Aufsichtsrat, Vorstand und Führungskräften, Führungskräften und Mitarbeitenden;
- nachhalten, dass die Führungskräfte die Werte der Risikokultur an die Mitarbeitenden kommunizieren;
- ein offenes und kollegiales Führungskonzept etablieren;
- transparente und nachhaltige Vergütungssysteme einrichten;
- für ein umfängliches Internes Kontrollsystem mit klaren Verantwortlichkeiten sorgen.

Allerdings endet das Thema Risikokultur nicht beim Vorstand, sondern alle Bereiche einer Bank einschließlich Aufsichtsrat sind Teil der Risikokultur und somit „mitverantwortlich“, wenn auch in unterschiedlichen Funktionen und Aufgaben:

Dem Aufsichtsrat obliegt die Pflege eines vertrauensvollen, offenen Austauschs im Gremium und mit dem Vorstand über die Beurteilung und Begrenzung der Risiken der Bank. Er soll Impulse für die Werte der Bank geben, beurteilen, ob der Vorstand die Risikopositionen richtig einschätzt und wie die risikominimierenden Prozesse oder Kontrollen ausgestaltet sind. Ganz allgemein ist es dabei die Aufgabe des Aufsichtsrats, zu prüfen, ob und welche Maßnahmen zur Schaffung und Förderung einer Risikokultur im Haus etabliert wurden.

Führungskräften als Bindeglied zwischen Geschäftsleitung und Mitarbeitenden kommt analog zum Vorstand eine Vorbildfunktion zu. Sie sollen zum einen das Wertesystem und die Risikolimits kennen und beachten und zum anderen das Wertesystem und die Risikokultur zu den Mitarbeitenden transportieren. Ihre Aufgabe im Kontext mit Risikokultur ist es, eine offene Kommunikation zu fördern, eine gute Fehlerkultur und Feedbackmöglichkeiten zu etablieren sowie die Risiken innerhalb ihrer Zuständigkeiten zu identifizieren, zu bewerten und zu kontrollieren. Dazu gehört aber auch, klare Verantwortlichkeiten festzulegen und den Mitarbeitenden die Konsequenzen etwaiger Verstöße zu kommunizieren.

Eine hervorgehobene Rolle kommt den Kontrolleinheiten zu. Sie sollen in besonderer Weise die Werte der Risikokultur vorleben und den Vorstand beraten und unterstützen.

Mitarbeitenden obliegt, das Wertesystem, den festgelegten Risikoappetit und die bestehenden Risikolimits in ihrem Verantwortungsbereich zu beachten und ihr Verhalten daran auszurichten sowie allgemein die relevanten Vorschriften zu kennen und zu beachten. Dazu gehört auch, zu hohe oder nicht gewünschte Risiken nicht einzugehen, risikominimierende Prozesse und/oder Kontrollen nicht zu umgehen und an (Pflicht-)Schulungen teilzunehmen. Ein Grundstein für die Implementierung einer wirksamen Risikokultur wird im Onboarding-Prozess gesetzt, da hier in der Regel der erste dauerhafte Kontakt zwischen Institut und (neuem) Mitarbeitendem erfolgt.

Für die notwendige Berichterstattung über die Risikokultur bietet sich der Jahresbericht des MaRisk-Compliance-Beauftragten an und/oder der Bericht im Zusammenhang mit dem operationellen Risiko seitens der Risikocontrolling-Funktion.[11]

Das Thema Risikokultur ist kein einmaliger Prozess, sondern ein regelmäßiger bzw. wiederkehrender Zyklus, insbesondere, wenn z. B. eine angestrebte „Ziel-Risikokultur“ noch nicht erreicht ist oder die Risikokultur noch nicht im angemessenen Umfang im Institut gelebt wird.[12]

Überwachung einer angemessenen Risikokultur in den Instituten

Im Rahmen der siebten MaRisk-Novelle im Jahr 2023 wurde das Thema Überwachung der Risikokultur auf allen Ebenen des Institutes in die MaRisk aufgenommen. Aufgabe des Vorstandes ist es somit auch, zu überwachen, ob durch die Mitarbeitenden die Risikokultur in ihrer täglichen Arbeit beachtet wird. Damit korrespondiert eine Rechenschaftspflicht der Mitarbeitenden gegenüber dem Vorstand hinsichtlich der Einhaltung der Risikokultur.[13] Wie eine Überwachung der Risikokultur innerhalb eines Hauses erfolgt, schreibt die Aufsicht nicht vor, insoweit gilt Methodenfreiheit. Es liegt im Ermessen der Institute, wie sie einen angemessenen Überwachungsprozess ausgestalten. Aus Institutssicht sollte es um eine effiziente Umsetzung der Risikokultur einschließlich Überwachung gehen. Dies kann beispielsweise durch Überwachung des Mitarbeitendenverhaltens in Bezug auf die Einhaltung der schriftlich fixierten Ordnung erfolgen, es bieten sich sowohl anlassbezogene als auch stichprobenartig durchgeführte Kontrollen an. Klassische Beispiele einer Überwachungshandlung für Risikokultur sind Mitarbeitendenbefragungen oder Selbstbewertungen in regelmäßigen Mit-arbeitergesprächen.

Praxisbeispiele der Risikokultur in den Instituten

In unserer Praxis als MaRisk-Compliance-Beauftragte beobachten und begleiten wir vielfältige gute Prozesse zur Risikokultur und deren Überwachung. Die nachfolgende Abbildung zeigt eine graphische Übersicht von Praxisbeispielen zu guter Risikokultur.

Aktuelle Entwicklungen

Die EZB hat in der zweiten Jahreshälfte 2024 ein Konsultationsverfahren zum Leitfaden „Governance und Risikokultur“ durchgeführt,[14] allerdings ist der für Mitte 2025 avisierte Leitfaden aktuell noch nicht veröffentlicht worden.[15] Es bleibt abzuwarten, ob und mit welchem Inhalt die EZB den Leitfaden veröffentlicht und wie die nationale Aufsicht damit umgeht.

Maßnahmen für die Etablierung und Förderung der Risikokultur in der Geschäfts- und Risikostrategie

Risikobegrenzende Kompetenzsysteme

- Risikoüberwachung mittels Zielkennzahlen / Schwellenwerten / Risikolimits
- Auswertung der Beschwerden und der Schadensfälle → Nachverfolgung der Maßnahmen

Transparente, konsequente – auf nachhaltige Erfolgsbeiträge ausgerichtete – Vergütungssysteme

Verhaltenskodex (Wertesystem)

- Zielvereinbarungs- und Zielerreichungsgespräche (die quantitativen/qualitativen Ziele verdeutlichen die Verantwortung des Einzelnen für die Gesamtheit und sind mit den Bankzielen verknüpft)
- Mitarbeiterentwicklungsgespräche
- Selbstbewertungen durch Mitarbeitende

Schulungen für neue Mitarbeitende zu risikoangemessenem Verhalten

- Mitarbeiterversammlung, Weekly, Town Hall Meeting
- Thematisierung der Risikokultur in den regelmäßigen Besprechungen der Teams/Abteilungen/Bereiche
- Entwicklung der Risikokultur z. B. als Bestandteil eines Strategieworkshops

- Mitarbeiterbefragungen („Wir-Gefühl“)
- Führungskräftebefragungen

Im Rahmen des Projekts „Geno Next Level“ wurde ein Vorstands- und Aufsichtsratskodex entwickelt, der in der Mitgliederversammlung des BVR im Jahr 2027 beschlossen werden soll.[16]

Zusammenfassung und Handlungsempfehlungen

Das Thema Risikokultur ist nicht neu, hat aufgrund von Ereignissen in der jüngsten Vergangenheit aber an Bedeutung gewonnen. Adressat einer angemessenen Risikokultur und verantwortlich für diese ist jeder in einem Institut: vom Azubi über den Vorstand bis hin zum Aufsichtsrat. Risikokultur lässt sich auch nur schwer in Zahlen messen und bedeutet nicht die Quantifizierung der wesentlichen Risiken. Risikokultur ist institutsindividuell und keine einmalige Aufgabe, sondern dauerhaft zu betrachten und zu gewährleisten, wobei es praxisbewährte Mittel zur Implementierung und Aufrechterhaltung einer angemessenen Risikokultur gibt. Sprechen Sie uns gerne an. ▬

Jörg Scharditzky
Abteilungsleiter MaRisk-Compliance,
E-Mail: joerg.scharditzky@dz-cp.de

Eugenia Scherbanev
Beauftragte MaRisk-Compliance,
E-Mail: eugenia.scherbanev@dz-cp.de

Thomas Schirmer
Beauftragter MaRisk-Compliance,
E-Mail: thomas.schirmer@dz-cp.de

[1] Und weiterer Skandale, z. B. Panama Papers und Cum/Ex- bzw. Cum/Cum-Geschäfte.

[2] BaFin-Rundschreiben 10/2012 (BA) vom 14.12.2012, Tz. AT 4.4.2 (https://www.bundesbank.de/resource/blob/598760/825c3c1518cdc5fce74f732fc0d05cc4/472B63F073F071307366337C94F8C870/2012-12-14-rundschreiben-data.pdf)

[3] Und die zuständigen Behörden in die Lage zu versetzen sind, sich der Angemessenheit der internen Unternehmensführungsregeln zu versichern; RL 2013/36/EU (Bankenrichtlinie – CRD IV) vom 26.06.2013, Rn. 54.

[4] Damit setzte die BaFin auch die Empfehlungen des Baseler Ausschusses für Bankenaufsicht aus dessen Prinzipen zur Corporate Governance aus dem Jahr 2015 um.

[5] Diese Definition baut auf einem Vorschlag des Financial Stability Board aus dem Jahr 2014 auf und wird auch in den EBA-Guidelines zur Internen Governance verwendet, EBA/GL/2021/05, 02.07.2021, S. 11, 14, 28.

[6] https://www.bundesbank.de/de/aufgaben/bankenaufsicht/einzelaspekte/aufsichtsschwerpunkte/schwerpunkte-der-bankenaufsicht-799612

[7] Formuliert bereits im Jahr 2014 vom Financial Stability Board (FSB) und ebenfalls in den EBA-Leitlinien wiedergegeben, EBA/GL/2021/05, 02.07.2021, S. 28 f.

[8] Hannemann u.a., MaRisk, TB 1, 2025, AT 3, Rn. 68

[9] Die Indikatoren stehen nicht isoliert da, sondern sind miteinander verzahnt, auch können institutseigene Indikatoren hinzukommen, z. B. Risikoappetit. Es kommt auch weniger auf eine Quantifizierung der Indikatoren an als auf eine qualitative Bewertung.

[10] MaRisk vom 27.10.2017, AT 3 Tz. 1

[11] Häufig wird der Risikocontrolling-Funktion die operative Verantwortung für die Umsetzung der Risikokultur übertragen, auf jeden Fall sollten das Risikocontrolling und die Compliance-Funktion beteiligt werden.

[12] Denkbar ist auch, einen andauernden „Regelkreis“ aufzusetzen.

[13] Hannemann u.a., MaRisk, TB 1, 2025, AT 3, Rn. 95

[14] Pressemitteilung der EZB vom 24.07.2024 (https://www.bundesbank.de/resource/blob/937238/bcdc155de32e6946d9cd2c2e386ba1b6/472B63F073F071307366337C94F8C870/2024-07-24-konsultationsverfahren-download.pdf)

[15] Dieser Artikel hat den Stand 20.01.2026.

[16] BVR-Roadshow 2026; https://intern.bvr.de/e.nsf/E21C0A31FAB9BA59C1258DB5004909BB/$FILE/BVR_Roadshow_Foliensatz.pdf