

# Risikokultur nach MaRisk – neue Anforderung ab 2018

## Warum jetzt und weshalb überhaupt?

MICHAEL SOMMA, DR. MAX WEBER, DIRK BRECHFELD

Die Novelle der Mindestanforderungen an das Risikomanagement (MaRisk) im Oktober 2017 hat das Thema Risikokultur im deutschen Aufsichtsrecht erstmals verankert. Die Umsetzungsfrist läuft zum 31. Oktober 2018 aus. Wenngleich es zunächst um die Verabschiedung, Dokumentation und bankinterne Kommunikation der Risikokultur geht, erwächst daraus die Überprüfung und Bewertung der gelebten Risikokultur. Der Beitrag beschreibt Besonderheiten für Finanzierungs-, Leasing- und Factoring-Geschäfte und gibt Anregungen zur Ausgestaltung. (Red.)

In den zurückliegenden zehn Jahren ist auf die Bankenbranche eine beispiellose Flut an neuen Regulierungsvorschriften sowie Verschärfungen bestehender Vorschriften zugekommen. Auslöser war die weltweite Finanzkrise und der daraus resultierende politische Wille, die Krisenresistenz der Finanzbranche zu stärken und den Einsatz von Steuergeldern zur Bewältigung künftiger Krisen zu vermeiden. So wurden beispielsweise die Eigenkapital- und Risikomessvorschriften auf allen

Ebenen erhöht.<sup>1</sup> Darüber hinaus ist eine Reihe neuartiger Regulierungsvorschriften auf den Weg gebracht worden wie etwa zu den Vergütungs- und Bonussystemen von Banken sowie zu Sanierungs- und Abwicklungsplänen.

- 1) Der Baseler Ausschuss hat in mehreren Schritten das Basel-II-Rahmenwerk erweitert und mit Verabschiedung der Basel-III-Finalisierung Ende 2017 abgeschlossen, wobei im Wesentlichen eine Umsetzungsfrist bis 2022 vorgesehen ist.
- 2) Vgl. Baseler Ausschuss: Corporate Governance Principles for Banks, BCBS 328, 2015.

Die Finanzkrise kann letzten Endes darauf zurückgeführt werden, dass vor allem international tätige Großbanken das wahre Ausmaß ihrer eingegangenen Risiken entweder zu gering und damit falsch eingeschätzt oder aber wider besseres Wissen in Kauf genommen hatten. Aus diesem Grund haben die Bankenaufsicher auf internationaler Ebene beschlossen, Banken in ihrem grundsätzlichen Umgang mit Risiken stärker denn je in die Pflicht zu nehmen und eine angemessene Risikokultur einzufordern.<sup>2</sup> Mit dem Thema Risikokultur verfolgen die Aufsicher das Ziel, auf allen Ebenen der Bank das Risikobewusstsein der Mitarbeiter, die Transparenz über die Risikobereitschaft der Bank und die zugehörigen Verhaltensregeln, Kontrollen und Entscheidungsprozesse zu stärken.

### Zahlreiche relevante Veröffentlichungen

Das Thema Risikokultur ist hierzulande erstmals mit der MaRisk-No-

#### DIE AUTOREN:

Michael Somma,  
Berlin,



Quelle: BfFach

leitet das Referat für Betriebswirtschaft beim Bankenfachverband e.V. Seit 2006 ist er Mitglied im Fachgremium MaRisk und begleitet in dieser Funktion die Weiterentwicklungen der MaRisk.

E-Mail: michael.somma@bfach.de

Dr. Max Weber,  
Stuttgart,



Quelle: EY

ist verantwortlicher Partner für EY im Bereich Risk Advisory (EMEIA Financial Services). Er leitet den Bereich Risikomanagement und ist seit fast 25 Jahren in der Beratung und Prüfung von Banken und Finanzdienstleistern im Bereich Aufsichtsrecht und Risikomanagement sowie bei Institutsgründungen tätig.

E-Mail: max.weber@de.ey.com

Dirk Brechfeld,  
München,



Quelle: EY

ist als Senior Manager für EY im Bereich Risk Advisory (EMEIA Financial Services) in aktuellen aufsichtsrechtlichen Themenstellungen der Finanzindustrie tätig und verantwortet vorrangig Umsetzungsprojekte im Governance-, Risiko- und Compliance-Umfeld.

E-Mail: dirk.brechfeld@de.ey.com

## Übersicht zu den aufsichtsrechtlich relevanten Veröffentlichungen

Herausgeber	Dokumente	Kernelemente
BaFin	▶ 5. MaRisk-Novelle vom 27. Oktober 2017	▶ Definition von Risikokultur, Verantwortung der Geschäftsführung (AT 3)
	▶ Anschreiben zur MaRisk-Konsultation 02/2016	▶ Verhaltenskodex
	▶ Risikokultur: Anforderungen an eine verantwortungsvolle Unternehmensführung (BaFin Journal August 2015)	▶ Bezugnahme auf die Indikatoren einer Risikokultur gemäß FSB (s.u.)
Financial Stability Board	▶ Guidance on Supervisory Interaction with Financial Institutions on Risk Culture: A Framework for Assessing Risk Culture (April 2014)	▶ Indikatoren einer soliden Risikokultur
	▶ Principles for An Effective Risk Appetite Framework (November 2013)	▶ Risikoappetit-Rahmenwerk, Risikolimits sowie Definition von Rollen und Zuständigkeiten
EBA	▶ Guidelines on common procedures and methodologies for the SREP ▶ Guidelines on internal governance (EBA/2017/11; ersetzt die bisherige/noch gültige EBA GL 44)	▶ Verantwortlichkeiten des Managements ▶ Anforderungen an Entscheidungsprozesse ▶ Bestandteile einer effizienten Kommunikation
Basel Committee on Banking Supervision	▶ Corporate governance principles for banks (BCBS 328)	▶ „Tone from the Top“ ▶ Definition Risikoappetit ▶ Verhaltenskodex
FCA	▶ Culture in Banking ▶ FCA Risk Outlook 2013	▶ Verantwortlichkeiten ▶ Whistleblowing
...	▶ ...	▶ ...

Quelle: EY Deutschland 2018

velle 2017<sup>3</sup> im deutschen Aufsichtsrecht verankert worden. Die zahlreichen, zuvor veröffentlichten internationalen und europäischen Papiere<sup>4</sup> waren bis zu diesem Zeitpunkt weitestgehend unbeachtet geblieben (siehe Abbildung). Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) hat die Ausführungen in den MaRisk vergleichsweise knapp gehalten. So bleibt beispielsweise die Frage, welche Erwartungen die BaFin mit Aufnahme des Themas Risikokultur in die MaRisk an die Institute richtet. Konkrete Ausgestaltungshinweise nennen die neuen MaRisk nämlich nicht.

Offenkundig ist, dass bei der neuen MaRisk-Anforderung zur Risikokultur nicht die Frage im Mittelpunkt steht, ob ein Institut eine solche hat oder benötigt. Jede Bank hat seit jeher eine eigene Risikokultur, ebenso wie eine eigene Unternehmenskultur, wozu auch die Risikokultur zählt. Im Mittelpunkt steht vielmehr die Frage, wie die Geschäftsleitung die Risikokultur im Sinne der strategischen

Ziele beeinflussen, kommunizieren, dokumentieren und vorleben kann. Im Hinblick auf die neuen MaRisk-Anforderungen zur Risikokultur räumt die BaFin den Banken bis zum 31. Oktober 2018 Zeit für die Umsetzung ein.

### Fünf Indikatoren einer Risikokultur

Zwar fordert das nationale Aufsichtsrecht mit den MaRisk eine Risikokultur, wie erwähnt fehlen auf nationaler Ebene (leider) jedoch jegliche Hinweise zur konkreten Ausgestaltung und Umsetzung. Insoweit ist die in der Übersicht aufgeführte „Guidance [...] on Risk Culture“ des Financial Stability Board (FSB) die derzeit am besten geeignete Grundlage zum umfassenden Verständnis der regulatorischen Anforderungen beziehungsweise Erwartungen an eine im Institut zu verankernde beziehungsweise vorhandene Risikokultur. Hieran lehnt sich auch die EBA-Leitlinie zur Internal Governance in ihrem

Titel IV, Tz. 94 ff. an. Eine angemessene Risikokultur wird laut FSB durch fünf<sup>5</sup> Indikatoren (Kernelemente) bestimmt, die sich in der bisherigen, nationalen Umsetzung so auch durchgesetzt haben. Diese fünf Indikatoren stellen die Kernelemente einer Risikokultur dar und beinhalten typischer Weise die folgenden, zentralen risikokulturellen Aspekte in Form von Leitlinien.

Vorgelebte Leitungskultur („Tone from the Top“/„Leadership“)

- ▶ „Tone from the Top“ – die Leitungsorgane haben eine Vorbildfunktion und leben das festgelegte Wertesystem im Sinne von „lead and influence“ vor.

3) Vgl. BaFin-Rundschreiben 09/2017 (BA) vom 27. Oktober 2017.

4) Neben dem Baseler Ausschuss haben vor allem das Financial Stability Board (FSB) und die Europäische Bankenaufsicht (EBA) eine Reihe von Papieren zur Risikokultur veröffentlicht.

5) Das FSB-Papier von 2014 definiert vier Indikatoren; zwischenzeitlich hat sich in der Umsetzungspraxis mit dem Themenblock „Risikomanagementrahmen“ ein weiterer, fünfter Indikator etabliert.

- Vom Management festgelegter Verhaltenskodex regelt, welches Verhalten in Bezug auf Risiken angestrebt wird.

Verbindliche Organisationsstruktur und Verantwortlichkeiten der Mitarbeiter („Accountability“)

- Klare Definition, Kommunikation sowie Verständnis von Rollen und Verantwortlichkeiten über alle „three lines of defence“. Aktivitäten jedes Mitarbeiters müssen im Einklang mit dem Wertesystem, dem Risikoappetit und den Risikolimits des Instituts stehen.
- Beachtung von Risiken im Rahmen von Entscheidungsprozessen führen zu ausgewogenen Entscheidungen. Mechanismen definieren die Verhaltensweise, die zur gewünschten Risikokultur führen soll.
- Die Geschäftsbereiche sind für die von ihnen eingegangenen Risiken verantwortlich.

Geeigneter Risikomanagementrahmen („Risk Framework inclusive Risk Appetite“)

- Der Risikoappetit ist durch die Leitungsorgane schriftlich definiert und berücksichtigt alle wesentlichen Risiken.
- Geeignete Indikatoren stellen sicher, dass das bestehende Risikorahmenwerk bekannt ist und beachtet wird. Ebenfalls wird sichergestellt, dass den Mitarbeitern die relevanten Implikationen aus dem Risikorahmenwerk (zum Beispiel dem Limitsystem) transparent gemacht werden.

Offene Kommunikation und kritischer Dialog („Effective Communication and Challenge“)

- Auf Basis definierter Kommunikationswege und -formen wird gewährleistet, dass zwischen der Geschäftsleitung und dem Aufsichtsorgan sowie gegenüber den übrigen Mitarbeitern ein transpa-

renter und offener Dialog stattfindet.

- Eine auf allen Ebenen erwünschte Äußerung alternativer Ansichten sowie Kritik zulassende beziehungsweise respektierende Einschätzungen werden gefördert.

Angemessene Anreizstrukturen („Incentives“)

- Eine materielle und/oder immaterielle Vergütungs- und Anreizstruktur dient dazu, die Mitarbeiter zu motivieren, sich dem Wertesystem und dem Verhaltenskodex im Institut entsprechend zu verhalten.
- Die Kriterien zur Leistungsmessung sind so festgelegt, dass die Mitarbeiter stets im Interesse des Instituts und im Einklang mit der Risikokultur handeln.

### Schlanke und angemessene Umsetzung

Jedes Institut verfügt über eine gelebte Unternehmenskultur, die zumindest implizit auch eine Risikokultur beinhaltet. Zudem finden sich zahlreiche Aspekte, die eine solche Kultur ausmachen, bereits in diversen Dokumenten, wie Strategien, Richtlinien, Rahmendokumenten et cetera wieder. Eine dokumentierte und gesamthafte Risikokultur ist beziehungsweise war jedoch zumeist nicht oder nicht mit sämtlichen vom FSB definierten Kernelementen vorhanden. Zudem ist fraglich, ob das, was als Risikokultur „gelebt“ wird, auch das ist, wie es „Tone from the Top“ gewünscht wird und sein sollte. Zu beobachten ist auch, dass die Vorgaben der Leitungsgremien mancherorts nicht mit den Risikomanagementvorgaben und den Anreizstrukturen kompatibel sind.

Die entscheidenden Fragestellungen der Umsetzung und Verankerung sind:

- Phase 1 „Soll“: Wie können und sollten im Rahmen des Vorhande-

nen schlanke Vorgaben gemacht und angemessen verankert werden?

- Phase 2 „Ist“: Wie kann das tatsächliche Agieren der Mitarbeiter bezogen auf das gewünschte Verhalten messbar gemacht und Maßnahmen abgeleitet werden?

Ein mögliches, praxisbewährtes Vorgehen für Phase 1 besteht darin, die Kernelemente in Form von Leitlinien in ein neu zu erstellendes Risikokultur-Rahmenwerk aufzunehmen. Idee dabei ist, ein neues Dokument zu erstellen und die bestehende schriftlich fixierte Ordnung (sFO) im Weiteren unverändert zu lassen. Dieses Rahmendokument braucht einen Umfang von rund zehn Seiten nicht zu überschreiten und kann in einem sehr schlanken Ansatz auch auf wenigen Seiten verfasst werden.

Um zu diesem Ergebnis zu kommen, sind zunächst die aufsichtsrechtlichen Vorgaben auf Basis der oben angegebenen Quellen in ein institutsspezifisches Soll zu überführen. Jedes Institut muss individuell entscheiden, welche Bestandteile es für sich als relevant erachtet und wie es diese Bestandteile interpretiert beziehungsweise umsetzt, da beispielsweise das Thema angemessene Anreiz- und Vergütungsstrukturen nur dann relevant ist, wenn solche Anreize wie Bonussysteme überhaupt vorhanden sind. Bei dieser ersten Aktivität wird somit innerhalb einer Expertenrunde (gegebenenfalls mit Beteiligung der Geschäftsführung) das institutsspezifische Sollbild einer Risikokultur hergeleitet.

Auf dieser Basis ist eine (dokumentarische) Gap-Analyse mittels der vorhandenen Dokumente durchzuführen, indem diverse Bestandteile der Risikokultur aus bestehenden Dokumenten „entliehen“ beziehungsweise auf diese referenziert werden. Bestandteile, die aktuell in keinem Dokument beschrieben sind beziehungsweise keinem bereits bestehenden Dokument sinnvoll zugeordnet werden können, sollten innerhalb des Rahmendokuments aufgenommen und erläutert werden. Am Ende steht

ein Rahmenwerk, das die Kernelemente und Leitlinien der institutspezifischen Risikokultur enthält, aufsichtskonform ist und mit den sonstigen Dokumenten (sFO) im Einklang steht.

Mit Abschluss dieser Phase 1 ist die institutsindividuelle Risikokultur zunächst „lediglich“ dokumentiert, verabschiedet und intern veröffentlicht. Das bedeutet aber noch nicht, dass die Mitarbeiter die Inhalte auch wirklich verinnerlicht haben und vorrangig auch danach handeln.

Zwingend ist mithin eine stetige Verankerung der zuvor definierten Risikokultur durch geeignete Kommunikations-, Trainings- und Unterstützungsmaßnahmen. Erst wenn diese Verankerungsmaßnahmen ausreichend Raum und Zeit eingenommen haben (ein bis zwei Jahre), macht der eigentliche Schwerpunkt von Phase 2, die Überprüfung und

Bewertung des tatsächlichen Verhaltens der Mitarbeiter gegen das gewünschte Zielbild in Form des institutsspezifischen Rahmendokumentes Risikokultur, Sinn.

Das heißt, die wesentlichen Bestandteile dieser Folgephase sind:

- ▶ Stetige Verankerung der in Phase 1 definierten Risikokultur durch geeignete Maßnahmen mittels angemessener Kommunikations-, Trainings- und Unterstützungsmaßnahmen. Zu den Unterstützungsmaßnahmen gehört auch eine klare Zuweisung und Kommunikation von Verantwortlichkeiten („accountability“).
- ▶ Entwicklung einer Methodik insbesondere durch Fragebögen und Workshops zur Messung der gelebten Risikokultur und Durchführung der Workshops und Einzelgespräche beziehungsweise Ausfüllen der Fragebögen zur Er-

mittlung von potenziellen Lücken zwischen dem festgelegten Zielbild und der gelebten Risikokultur im Institut.

- ▶ Entwicklung und Implementierung eines Konzepts zur Schließung der erkannten Lücken.

Dabei steht die Frage im Mittelpunkt, wie sich die Mitarbeiter in spezifischen Situationen im Abgleich zu den Leitplanken der dokumentierten Risikokultur tatsächlich verhalten.

Die Phase 1 „Risikokultur-Rahmenwerk“ sollte den nationalen Vorgaben folgend noch in diesem Jahr abgeschlossen werden.<sup>6</sup> Die Um-

6) Für alle Neuerungen der MaRisk-Novelle 2017 ist ein formale Umsetzungsfrist bis 31. Oktober 2018 vorgesehen; da die Etablierung einer institutsindividuellen Risikokultur dem Charakter nach nie abgeschlossen ist, legen die Autoren die unspezifischen Anforderungen so aus, dass (zumindest) die Ausarbeitung des „Risikokultur-Rahmenwerks“ innerhalb der gesetzten Frist erfolgt sein sollte.



**efcom**

**Maßgeschneiderte  
Factoringsoftware.**



[www.efcom.de](http://www.efcom.de)

setzung gemäß Phase 2 macht dem vorgestellten Ansatz folgend erst im Anschluss und nach stetiger Verankerung risikokulturellen Verhaltens Sinn, das bedeutet über die nächsten Jahre.

### Finanzierung, Leasing, Factoring – Besonderheiten

Als Teil einer umfassenden „Corporate Culture“ ist die Risikokultur auf die spezifischen Risiken im Handeln des jeweiligen Instituts durch seine Leitungsfunktion und Mitarbeiter ausgerichtet. Diesem Leitgedanken folgend sollten sich in der jeweiligen Risikokultur solche Elemente und Aussagen wiederfinden, die die spezifischen Risiken des Unternehmens und seiner Branchenzugehörigkeit determinieren, wie nachfolgend beispielhaft dargestellt.

#### Finanzierung

- ▶ Beispiel Leitungskultur: Stetige Betonung („Tone from the Top“), dass die Mitarbeiter der Kunden- und Marktfunktionen als sogenannte erste Verteidigungslinie verantwortlich für die eingegangenen Risiken beispielsweise Adressenausfallrisiken sind; die zweite Verteidigungslinie (Risikoccontrolling-/Compliance-Funktion) agiert vorrangig in der „systemischen“ Verantwortung für das jeweilige Risiko- beziehungsweise Compliance-Management-System.

- 7) Abzuleiten aus der gesonderten Hervorhebung gemäß §§ 24a Absatz 3c und 25k Absatz 2 Kreditwesengesetz.
- 8) Zur Unterstützung seiner Mitgliedsbanken hat der Bankenfachverband in Kooperation mit EY eine „Bauanleitung zur Erstellung eines Rahmendokuments Risikokultur“ entwickelt und veröffentlicht, [www.bfach.de](http://www.bfach.de). Dieser Leitfaden stellt praxisorientiert die notwendigen Schritte zur Definition einer institutsspezifischen Risikokultur und zur Erstellung eines individuellen Rahmendokuments dar.
- 9) Die deutsche Aufsicht ist mit der Neuausrichtung ihres Leitfadens „Aufsichtliche Beurteilung bankinterner Risikotragfähigkeitskonzepte und deren prozessualer Einbindung in die Gesamtbanksteuerung („ICAAP“)“ im Mai 2018 von ihrem bisherigen Konzept abgerückt und hat die europäischen Entwicklungen adaptiert.

- ▶ Beispiel Organisationsstruktur: Definition eines klaren Rollen- und Risikoverständnisses jedes Mitarbeiters inklusive Vorgaben (Kompetenzen, Limitsystem et cetera) mit eindeutigen Funktionstrennungen zwischen Markt, Marktfolge, Backoffice et cetera wie auch über die „Drei Verteidigungslinien“ hinweg; Cooling-Off-Vorgaben bei Wechsel von Mitarbeitern über die Verteidigungslinien hinweg.

#### Leasing

- ▶ Beispiel Risikomanagementrahmen: Besondere Thematisierung der spezifischen Restwert-/Objekt-Risiken des Leasing-Geschäftes im Rahmen der Risikokultur; beispielsweise Begrenzung dieser Risiken durch Fokussierung auf bestimmte (nur wenige) Leasing-Objekte, Einschränkung der Nutzungsmöglichkeiten der Leasing-Objekte, stringente (risikorelevante) Auswahl der Leasing-Nehmer et cetera. Hierzu bedarf es klarer und expliziter Aussagen im Rahmen der Festlegung des Risikoappetits in Bezug auf das Restwertisiko.
- ▶ Beispiel Anreizstrukturen: Zeitliche Auszahlungsschranken beziehungsweise Bindung von Vertriebsprovisionen an Laufzeit und Erfüllung der Leasing-Verträge.

#### Factoring

- ▶ Beispiel Kommunikation: Offene Kommunikation und Sensibilisierung, dass das Factoring-Geschäft aufgrund des typischen Drei-Parteien-Verhältnisses und insbesondere bei grenzüberschreitender Tätigkeit erhöhten Geldwäsche-risiken unterliegt.<sup>7</sup>
- ▶ Beispiel Risikomanagementrahmen: Besondere Thematisierung der Risiken in Bezug auf die Anschlusskunden im Risikoappetit und in den weiteren Risikomanagementverfahren, verbunden mit einem klaren „Tone from the Top“ hinsichtlich der Bedeutung

der Bonität und Kreditwürdigkeit der Anschlusskunden.

Diese Beispiele möglicher Indikatorenprägungen mögen als Anregung zur weiteren Vertiefung dienen und verdeutlichen, dass die Festschreibung nicht trivial ist und sich eines generellen „One-size-fits-all-Ansatzes“ entzieht. Die Risikokultur ist so individuell wie das Unternehmen selbst.

### Entwicklung bleibt spannend

Mit Aufnahme des Themas Risikokultur in die MaRisk im Jahr 2017 und Gewährung einer Umsetzungsfrist bis Oktober 2018 ist die deutsche Aufsicht im europäischen Vergleich tendenziell eher „Nachzügler“. Dennoch sollten Banken nicht die Bedeutung unterschätzen, welche die BaFin dem Thema Risikokultur beimisst.

Derzeit liegt der Fokus zwar auf der Verabschiedung, Dokumentation und bankinternen Kommunikation der Risikokultur (Phase 1). Diese Phase kann bei einem strukturierten Vorgehen mit überschaubarem Aufwand und Kapazitäteneinsatz effizient abgearbeitet werden.<sup>8</sup>

Die aufsichtliche Erwartungshaltung wird jedoch in den kommenden Jahren steigen und eine Überprüfung und Bewertung der tatsächlich gelebten Risikokultur erforderlich machen (Phase 2). Ein Vorreiter bei diesem Thema ist die niederländische Aufsicht, die bereits heute die „gelebte“ Risikokultur in Banken unter Hinzuziehung von Psychologen intensiv prüft und dezidiert bewertet. Es ist davon auszugehen, dass nicht nur die Europäische Zentralbank derartige Entwicklungen mit hohem Interesse verfolgt. Auch die BaFin entwickelt ihre Prüfungsmaßstäbe stetig weiter und orientiert sich zunehmend an europäischen Vorgaben, wie nicht zuletzt das Thema Risikotragfähigkeit verdeutlicht.<sup>9</sup> ◀