FIRM
Frankfurter Institut für
Risikomanagement und Regulierung

FIRM Positionspapier Nr. 1 – November 2022

Risikokultur – Perspektiven zum aufsichtlichen Fokus und zur gelebten Praxis in den Instituten

DAS WICHTIGSTE AUF EINEN BLICK

Eine robuste Risikokultur ist als Bestandteil von Unternehmenskultur und guter Corporate Governance ein Erfolgsfaktor – das haben viele Banken schon früh erkannt. Spätestens mit der Beschäftigung der Regulatoren mit diesem Thema und der folgerichtigen Aufnahme expliziter Anforderungen in die CRR sowie weitere aufsichtsrechtliche Dokumente ist das Thema in der Breite der Branche angekommen.

Leitungskultur („Tone from the Top"), Verantwortlichkeiten, wirksame Kommunikation und kritischer Dialog sowie Anreize: Diese Kernbausteine der Risikokultur sind inzwischen als theoretisches Konstrukt etabliert. Die hieraus vom Arbeitskreis „Risikokultur" des Frankfurter Instituts für Risikomanagement und Regulierung (FIRM) abgeleiteten zehn Thesen lassen sich durch eine Befragung der Mitgliedsinstitute jedoch nur teilweise bestätigen.[1] Während die Konzeption einer Risikokultur (mit Ausnahme einzelner Themen wie z. B. Zielvereinbarungssysteme) recht weit fortgeschritten zu sein scheint, gibt es bei der Operationalisierung in vielen Instituten noch Handlungsbedarf.

In der Corona-Pandemie hat sich gezeigt, inwiefern Banken von einer robusten, etablierten Risikokultur profitieren können. Angesichts weiterer aktueller und zu erwartender Störfaktoren (geopolitische Krisen, Klimawandel etc.) bleibt die Resilienz im Finanzwesen weiter wichtig. Eine passgenaue Risikokultur kann ein wesentlicher Baustein hierfür sein – nicht nur als Beitrag zur Erfüllung aufsichtsrechtlicher Anforderungen, sondern auch als potenzieller Wettbewerbsvorteil.

EINFÜHRUNG

Schon die Finanzmarktkrise 2008 hat deutlich gezeigt: Eher mechanistisch ausgerichtete Regelwerke, wie sie beispielsweise in Säule I von Basel II oder im „Three Lines of Defense"-Ansatz vorgegeben werden, reichen allein nicht aus, um die Widerstandsfähigkeit von Banken gegenüber veränderten Risiken zu stärken. Diese Widerstandsfähigkeit wird allerdings wichtiger angesichts einer Risikolandschaft, die sich immer schneller verändert – mit Themen wie Cyberkriminalität und Kryptowährungen/-anlagen, Klimarisiken und territorialen Konflikten. Zudem haben sich etablierte Regelwerke oft nicht als hinreichend geeignet erwiesen, adäquate Anreize zu setzen, um andere Unternehmensziele wie beispielsweise das Gewinnstreben angemessen zu gewichten.

Die Aufsichtsbehörden haben in den vergangenen zehn Jahren die Risikokultur als Teil der Governance in den Fokus gerückt. Im Folgenden stellen wir in einem Kurzabriss zum aufsichtlichen „Risikokultur"-Konzept (Kapitel 1) zunächst dar, über welche Normen die Aufsicht[2] einen prinzipienbasierten Ansatz zur Stärkung und letztlich auch Überwachung der Risikokultur vorgibt.

Vor diesem Hintergrund stellen wir in Kapitel 2 die Kernergebnisse einer aktuellen Umfrage des Frankfurter Instituts für Risikomanagement und Regulierung (FIRM) zum Status quo der Risikokultur in Kreditinstituten in Deutschland und Österreich vor; Kapitel 3 gibt abschließend einen Ausblick auf die Vorteile einer robusten Risikokultur in Zeiten der Covid-19-Pandemie und anderer Krisen.

1. KURZABRISS: DAS AUFSICHTLICHE „RISIKOKULTUR"-KONZEPT

Der prinzipienbasierte Ansatz der Aufsicht zur Stärkung und letztlich auch Überwachung der Risikokultur benennt relevante Elemente einer Risikokultur und stellt, wo immer dies möglich ist, eine Verbindung zu bereits etablierten Konzepten wie dem Risikoappetit und der Risikostrategie oder dem ILAAP/ICAAP her. Damit können Banken eine für ihr Geschäftsmodell passende

1 Parallel zu der hier dargestellten Umfrage zur Risikokultur hat FIRM deutsche Institute zu ihren Risikoappetitframeworks für nicht-finanzielle Risiken befragt, um den Status Quo und die Handlungsschwerpunkte zu bestimmen und zu vergleichen – die Ergebnisse und Ableitung daraus lassen sich in einem zweiten FIRM Positionspapier finden: FIRM Positionspapier Nr. 2 – November 2022: FIRM-Befragung zu Risikoappetit Frameworks für nicht-finanzielle Risiken: Status Quo und Handlungsschwerpunkte im Bankensektor

2 Mit dem Begriff „Aufsicht" sind im Folgenden nicht nur die Institutionen des SSM (BaFin, EBA, EZB) gemeint, sondern auch die Institutionen, in denen sich die Aufsichtsbehörden organisieren (FSB, BCBS). Inkludiert sind zudem Anforderungen der Aufsicht, die sich aus der Referenz auf Publikationen internationaler Organisationen wie etwa G30 und IIF ergeben.

Risikokultur aufsetzen und weiterentwickeln, ohne dass Widersprüche zu anderen aufsichtlichen Konzepten entstehen. Darüber hinaus ist die Auseinandersetzung mit den internationalen Organisationen der Banken zur Abrundung des Anforderungsbilds zu empfehlen. Denn „grundsätzlich ist die richtige Kultur und das richtige Verhalten nicht nur eine aufsichtsrechtliche Anforderung. Sie ist notwendig für die wirtschaftliche und soziale Nachhaltigkeit der Banken und des Bankwesens" [G30 2018].

Die folgenden Abschnitte beschreiben Risikokultur als Element des Governance Framework sowie die aufsichtlichen Erwartungen zum einen an die wichtigsten Stakeholder der Risikokultur und zum anderen an die Maßnahmen zu ihrer Stärkung.

1.1 RISIKOKULTUR ALS ELEMENT DES GOVERNANCE FRAMEWORK

Die EU-Eigenkapitalrichtlinie von 2013 gibt den EU-Mitgliedsstaaten unter anderem vor, dass sie "Grundsätze und Standards einführen, die (...) eine robuste Risikokultur auf allen Ebenen von Kreditinstituten und Wertpapierfirmen fördern"[EU 2013]. Damit greift die EU-Richtlinie den Begriff Risikokultur auf, der zuvor bereits in einzelnen Veröffentlichungen des Baseler Ausschusses und anderer Organisationen verwendet wurde, die sich mit Bankenregulierung beschäftigen.

Der Begriff Risikokultur adressiert den Teil der Unternehmenskultur, der sich auf Risikobewusstsein, Risikoübernahme und Risikomanagement bezieht [BCBS 2015], und wird sowohl vom FSB als auch vom Baseler Ausschuss und von der EBA wie folgt definiert:

„(Risikokultur umfasst) die Normen, Einstellungen und Verhaltensweisen eines Instituts in Zusammenhang mit Risikobewusstsein, Risikobereitschaft und Risikomanagement sowie den Kontrollen, die für Entscheidungen über Risiken maßgeblich sind. Die Risikokultur beeinflusst die Entscheidungen der Geschäftsleitung und der Mitarbeiter im Tagesgeschäft und hat Auswirkungen auf die Risiken, die sie eingehen". [EBA 2021]

Entsprechend sind die Risikokultur sowie die Maßnahmen zur Gestaltung und Förderung einer robusten Risikokultur Bestandteil des Governance Framework von Banken (**Schaubild 1**).

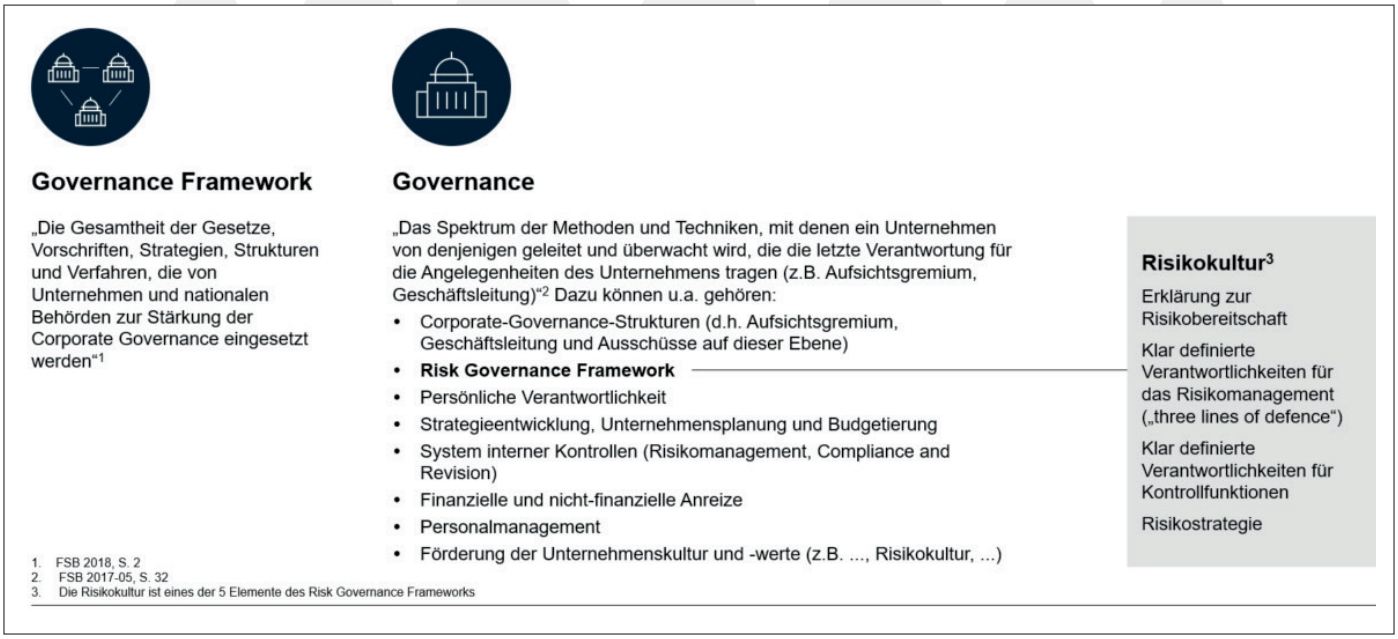
Dass die Risikokultur einerseits breite Auswirkungen auf die weiteren Elemente des Risk Governance Framework hat, ergibt sich zwangsläufig aus ihrer Funktion per Definition. Gesondert zu erwähnen ist hier jedoch, dass die Risikokultur als entscheidende Voraussetzung für ein robustes Risikomanagement angesehen wird [ECB 2016].

Andererseits wird die Risikokultur ihrerseits von den (meisten) anderen Elementen des Risk Governance Framework beeinflusst. Das FSB hebt dabei insbesondere hervor, dass eine robuste Risikokultur durch eine effektive Risk Governance, ein „Risk Appetite"-Framework und Vergütungsregelungen, unterstützt wird, die angemessenes Verhalten bei der Risikoübernahme fördern [FSB 2014].

1.2 ÜBERBLICK ZU DEN AUFSICHTLICHEN ERWARTUNGEN AN DIE STAKEHOLDER DER RISIKOKULTUR

Die Anforderungen des einheitlichen europäischen Bankenaufsichtsmechanismus an die Risikokultur hat die EBA 2021 in

SCHAUBILD 1



Grafik: FSB, BCBS, EBA, eigene Darstellung (Einzelquellen in der Grafik)

ihrem finalen Report über die Leitlinien zur internen Governance fixiert [EBA 2021]. Sie fordern von der Geschäftsleitung, eine Risikokultur zu etablieren, die das Risikobewusstsein und das Risikoübernahmeverhalten des Instituts adressiert. Dabei soll die Umsetzung der Risikokultur auf Geschäftsleitungsebene festgelegt, genehmigt und überwacht werden.

Schlüsselelement der Risikokultur ist die Erwartung, dass sich alle Mitarbeitenden konform zu geltenden Rechts- und internen Vorschriften verhalten und ethisch arbeiten. Entsprechend werden einerseits individuelle Integrität und die Zielsetzung gefordert, faire Ergebnisse für die Kunden anzustreben, während andererseits beobachtetes Fehlverhalten innerhalb oder außerhalb der Organisation unverzüglich zu eskalieren ist [FSB 2014]. Darüber hinaus soll die Risikokultur grundsätzlich zu den Werten einer Bank passen, die ihrer Sorgfaltspflicht nachkommt, etwa im Kontext von Geldwäscheprävention und Abwehr von Terrorismusfinanzierung. Und nicht zuletzt soll sie eine offene bidirektionale und bereichsübergreifende Kommunikation im Unternehmen fördern.

Zusätzlich resultieren Erwartungen an die Risikokultur aus den Anforderungen an die Unternehmenskultur, da die Risikokultur von der Aufsicht als Bestandteil sowohl der Unternehmenskultur als auch der Corporate Governance angesehen wird [BCBS 2015; FSB 2017]. An die Corporate Governance hegt die Aufsicht nicht nur abstrakte Erwartungen, sondern stellt auch konkrete inhaltliche Anforderungen:

„Vorrangiges Ziel der Corporate Governance sollte es sein, die Interessen der Stakeholder im Einklang mit dem öffentlichen Interesse nachhaltig zu wahren. Unter den Stakeholdern, insbesondere bei Retail-Banken, sind die Interessen der Aktionäre den Interessen der Einleger untergeordnet." [BCBS 2015]

Von einer robusten Risikokultur wird dementsprechend erwartet, dass sie das Risikobewusstsein sowie die Angemessenheit von Beurteilung und Verhalten bei der Risikoübernahme unterstützt. Dazu hat sie sicherzustellen, dass sich abzeichnende Risikoentwicklungen erkannt, analysiert, eskaliert und adressiert werden [FSB 2014]. Eine robuste Risikokultur unterstreicht somit erstens die Bedeutung

- eines angemessenen Risiko-Rendite-Verhältnisses
- eines effektiven Kontrollsystems
- von Risikomodell-Qualität und Datengenauigkeit sowie des Hinterfragens von Risikoübernahme-Entscheidungen
- der Nachverfolgung von Limitüberschreitungen und operativen Vorkommnissen, bei Bedarf mit disziplinarischen Maßnahmen
- von horizontaler und vertikaler offener Kommunikation im Unternehmen, insbesondere der frühzeitigen Einbeziehung der Kontrollfunktionen in die Pläne der Geschäftsleitung [FSB 2014; BCBS 2015].

Zweitens ist eine robuste Risikokultur auch eine wichtige Voraussetzung zur Begrenzung des Fehlverhaltensrisikos [FSB 2018]. Bemerkenswert ist zudem, dass die Aufsicht dem obersten (Aufsichts)Organ von Banken umfassende Verantwortung überträgt, vor allem

- das Einnehmen einer führenden Rolle bei der Festlegung von Unternehmenskultur und Werten der Bank
- die Überwachung der Vergütungsstruktur einschließlich einer Beurteilung, ob diese mit der Risikokultur und der Risikobereitschaft der Bank in Einklang steht
- die Überwachung der Grundsätze und Verfahren der Bank für das Whistleblowing
- die Umsetzung der erforderlichen Führungskultur [BCBS 2015].

Weitere Anforderungen werden gestellt an die Geschäftsleitung, den CRO und die Wirtschaftsprüfer:

- Die **Geschäftsleitung** ist gefordert, einen schriftlich fixierten Verhaltenskodex für die Mitarbeiter zu entwickeln [BCBS 2015]. Gemäß MaRisk AT5 ist dies für kleine, wenig komplexe Kreditinstitute allerdings nicht zwingend erforderlich [BaFin 2021].
- Der **CRO** ist vorbehaltlich der Überprüfung und Genehmigung durch das oberste Verwaltungsorgan dafür zuständig, den unternehmensweiten Rahmen für die Risikosteuerung zu entwickeln und umzusetzen, der die Risikokultur, die Risikobereitschaft und die Risikolimite der Bank umfasst [BCBS 2015]. Zudem ist er verantwortlich für Prüfung und Beurteilung der Internal Governance (unter anderem ein SREP-Schlüsselelement) [ECB 2016]. Dies schließt insbesondere die Beurteilung der Risikokultur mit ein [BCBS 2015].
- In den einschlägigen Werken der **Wirtschaftsprüfer** wird die Risikokultur ebenfalls thematisiert [IDW 2022] bzw. werden ihre wesentlichen Elemente beschrieben [WPH 2020]. Bei diesen Ausführungen von geringem Umfang handelt es sich allerdings nur um Hinweise zur weiteren Beschäftigung mit den aufsichtsrechtlichen Anforderungen.

1.3 AUFSICHTLICH ERWARTETE MASSNAHMEN ZUR VERBESSERUNG DER RISIKOKULTUR

Welche Maßnahmen von der Aufsicht gefordert werden, lässt sich sowohl aus direkten Empfehlungen als auch aus den

Prüfungsleitlinien der aufsichtlichen Institutionen ableiten. Das FSB hat hierzu bereits 2014 eine Sammlung von Maßnahmen bzw. Indizien für eine robuste Risikokultur veröffentlicht [FSB 2014]. Zusätzlich zu den in Kapitel 1.2 genannten drei Elementen Risk Governance, Risk Appetite Framework und Vergütungsregelungen werden darin zahlreiche weitere Maßnahmen bzw. Indikatoren in den vier Kategorien Leitungskultur („Tone from the Top"), Verantwortlichkeiten, wirksame Kommunikation/ kritischer Dialog und Anreize erwähnt. Im Folgenden ist für jede der vier Kategorien erläutert, welche Anforderungen bzw. umgesetzten Maßnahmen vorrangig erwartet werden.

Leitungskultur („Tone from the Top")

- Aufsichtsgremium und Geschäftsleitung haben eine klare Vorstellung von der angestrebten Risikokultur und deren Auswirkungen auf das Institut. Sie überwachen und bewerten die existierende Risikokultur und adressieren identifizierte Schwachstellen.

- Es gibt Mechanismen wie z.B. vertrauliche 360-Grad-Bewertungsprozesse, die sicherstellen, dass die Entscheidungsfindung nicht von einer einzelnen Person oder einer kleinen Gruppe von Personen in einer Weise dominiert wird, die den Interessen der Institution als Ganzes schadet.

- Für die Geschäftsleitung gelten dieselben Anforderungen in Bezug auf Integrität, Risikobeherrschung und Risikokultur wie für alle anderen Mitarbeitenden.

- Das Aufsichtsgremium und die Geschäftsleitung bewerten systematisch, ob die vertretenen Werte von Management und Mitarbeitenden auf allen Ebenen kommuniziert und proaktiv gefördert werden, so dass der „Tone in the Middle" mit dem „Tone from the Top" übereinstimmt.

- Es sind geeignete Mechanismen vorhanden, um sicherzustellen, dass die Risikobereitschaft, die Risikomanagementstrategie und die Geschäftsstrategie wirksam aufeinander abgestimmt und in die Entscheidungsfindung und die Abläufe auf allen relevanten Ebenen des Instituts eingebettet sind.

- Es gibt Verfahren, mit denen Mängel im Risikomanagement auf den entsprechenden Leitungsebenen des Instituts überprüft werden, um die Ursachen für die Mängel zu ermitteln und die Gelegenheit zu nutzen, die Risikokultur des Finanzinstituts zu stärken.

Verantwortlichkeiten

- Die Verantwortung für Risiken ist eindeutig geregelt. Es gibt klare Anforderungen an Geschäftsbereiche, Geschäftsleitung und Aufsichtsgremium hinsichtlich Überwachung und Reporting von aktuellen und sich abzeichnenden Risiken sowie das Reagieren darauf. Die primäre Verantwortung für das Verhaltensrisiko ist auf die erste Verteidigungslinie verlagert worden, um sicherzustellen, dass das Verhaltensrisiko tatsächlich vom Unternehmen getragen wird und die erste Verteidigungslinie effektiv ist [GS30 2018].

- Angemessene Eskalationsprozesse zur Unterstützung des Risikomanagements sind etabliert. Es gibt systematische Auswertungen zum Wissen der Beschäftigten über die Eskalationsprozesse und zu ihrer Einschätzung der Offenheit im Institut für kritisches Hinterfragen.

- Die Konsequenzen exzessiver Risikoübernahme sind für alle Beteiligten klar und werden gezogen. Verstöße gegen interne Vorschriften, Risikolimite und den Verhaltenskodex haben grundsätzlich Konsequenzen für Vergütung und Karriere.

- Zusätzlich zur Rechenschaftspflicht der Mitarbeiter für ihr Risikoverhalten, fällt die Überwachung der Risikokultur und ihrer Einhaltung auf allen Ebenen explizit in die Verantwortung der Geschäftsleiter, welche bei beobachteten Mängeln frühzeitig mit klaren, ergebnisorientieren Maßnahmen reagieren müssen [MaRisk 2022]

Wirksame Kommunikation und kritischer Dialog

- Offene Kommunikation und das Äußern abweichender Meinungen werden gefördert. Zudem wird regelmäßig überprüft, inwiefern offene Kommunikation und kritisches Hinterfragen in die Entscheidungsprozesse integriert sind.

- Die Kontrollfunktionen sind gleichberechtigt mit den Geschäftsbereichen, sind in den Ausschüssen vertreten und werden in die relevanten Risikoaktivitäten einbezogen. Sie haben Zugang zum Aufsichtsgremium und zur Geschäftsleitung und agieren nicht nur als Berater, sondern übernehmen auch Kontrollfunktionen in Bezug auf die Risikokultur [FSB 2014].

Anreize

- Unter den Anreizen sind zahlreiche Maßnahmen erfasst, die über die bloße Beschränkung der Ergebnisabhängigkeit von

Gehältern hinausgehen. Denn nicht nur die Vergütungspraxis ist ein wichtiger Treiber des Verhaltens in den Banken, sondern auch die nichtfinanziellen Incentives [FSB 2018].

- Leistungsmessung und Vergütungsregelungen berücksichtigen systematisch die individuelle und gruppenweite Einhaltung der Grundwerte und der Risikokultur des Finanzinstituts. Beide incentivieren die Mitarbeiter, im Interesse des gesamten Unternehmens zu handeln und nicht nur für sich selbst oder ihren Geschäftsbereich [FSB 2014].

- Nachfolgeplanungen berücksichtigen nicht nur ertragsbasierte Leistungen, sondern auch persönliche Risikomanagement-Erfahrungen [FSB 2014].

- Maßnahmen in der Personalentwicklung umfassen das Definieren des Verständnisses von Risikomanagement und Unternehmenskultur als wesentliche Skills für leitende Positionen, Jobrotation zwischen Kontrollfunktionen und Geschäftseinheiten sowie Trainingsangebote für alle Mitarbeiter zu Risikomanagement, offener Kommunikation und anderen Elementen einer robusten Risikokultur [FSB 2014].

2. KERNERGEBNISSE DER FIRM-UMFRAGE ZUR RISIKOKULTUR IN BANKEN

Das Frankfurter Institut für Risikomanagement und Regulierung (FIRM) hat Ende 2021 eine Umfrage zur Risikokultur unter repräsentativen[3] Kreditinstituten in Deutschland und Österreich durchgeführt (siehe **Textbox 1**).[4] Zwei Aspekte sollten beleuchtet werden: erstens, wie Banken aktuell an das Thema Risikokultur herangehen und es konzeptionell behandeln, und zweitens, wie die gegenwärtig gelebte Praxis der Risikokultur in den Kreditinstituten aussieht. Zudem zielte die Umfrage darauf ab, zehn zentrale Hypothesen des FIRM-Arbeitskreises „Risikokultur" zu validieren und Verbesserungsfelder zu identifizieren.

Im Folgenden beschreiben wir – ausgehend von den Ergebnissen der Umfrage – den Status quo bei der „Risikokultur"-Definition, bei den operativen Verantwortlichkeiten im „Risikokultur"-Kontext, bei Bewertung, Reporting und Kommunikation der Risikokultur sowie bei den Stärken und Schwächen ihrer Ausgestaltung.

Textbox 1

Teilnehmer und Themenfelder der Umfrage

Mit ca. 20 befragten Instituten in Deutschland und Österreich umfasst die Umfrage ca. 44 %[5] der Bilanzsumme des deutschen Bankensektors und zählt acht der zehn größten deutschen Banken zu den Teilnehmern. Zudem wurde auf Grund der unterschiedlichen Charakteristika der Teilnehmer insgesamt ein breites Spektrum der Bankenlandschaft abgebildet: Ein Drittel der Institute wies eine Bilanzsumme von jeweils mehr als 200 Mrd. EUR auf, die Bilanzsummen der übrigen Institute lagen zwischen 1 Mrd. EUR und 190 Mrd. EUR. Zudem nahmen unterschiedliche Typen von Banken an der Umfrage teil – unter anderem Universal-, Landes- und Förderbanken.

Die Umfrage richtete sich explizit an Risikovorstände bzw. deren Bereichsleitung und umfasste mehr als 20 offenen und geschlossenen Fragen. Abgefragt und bewertet wurden entlang vordefinierter Kerndimensionen der Risikokultur die Definitionen, Verhaltensmuster, Prozesse, formalen Regel- und Richtliniendefinitionen sowie Zielbilder, Maßnahmen und Ansätze zur konkreten Ausgestaltung. Zusätzlich wurden die Effekte der COVID-19-Pandemie auf die Risikokultur beleuchtet. Alle Teilnehmer wurden gebeten, Weiterentwicklungs- und Gestaltungsvorschläge und somit auch eine weiterführende Perspektive auf das Thema zu teilen. Dadurch wurde auch eine Validierung der zehn Thesen zur Risikokultur möglich, die vom FIRM-Arbeitskreis vorab aufgestellt wurden:

These 1: Risikokultur manifestiert sich in verschiedenen Elementen einer Organisation, beispielsweise in Chance-Risiko-Abwägungen bei Entscheidungen.

These 2: Risikokultur ist in die Organisationskultur eines Unternehmens eingebettet. Die Fehlerkultur ist dabei ein Teilelement der Risikokultur; Compliance- und Risikokultur überlappen sich.

These 3: Eine durchlässige Organisationsstruktur, funktionierende Prozesse, fest verankerte Werte sowie das angemessene Verhalten des Einzelnen bilden die Grundfeste einer robusten Risikokultur.

These 4: Risikokultur bedarf einer Balance zwischen Formalisierung und Freiheitsgraden, um die Entscheidungsfähigkeit des Einzelnen sicherzustellen.

These 5: Die Kongruenz von Wort und Tat stellt ein wesentliches Element einer robusten Risikokultur dar.

3 Die Institute, die an der Umfrage teilnahmen, sind identisch mit denen, die sich bei FIRM engagieren. Dadurch wird eine gute Grundgesamtheit abgebildet.

4 Die Umfrage wurde im Auftrag des Arbeitskreises „Risikokultur" des FIRM durchgeführt.

5 Der Anteil der befragten Institute aus Österreich an der Bilanzsumme des österreichischen Bankensektors hingegen liegt bei < 5%.

These 6: Eine klare und leicht verständliche Sprache (innerhalb der Organisation und auch als „Tone from the Top"), eindeutig formulierte Erwartungen sowie die Konsistenz der gesendeten Botschaften über Zeit unterstützen die Risikokultur.

These 7: Über gezielte Anreize (nicht nur monetärer Art) und Interventionen lässt sich die Risikokultur immer wieder in das Bewusstsein des Einzelnen holen sowie gezielt stärken.

These 8: Das Akzeptieren von Fehlern, das Lernen aus Fehlern sowie das Feedback des Gelernten zurück in die Organisation fördern eine starke Risikokultur.

These 9: Angemessene Sanktionen und Konsequenzen fungieren innerhalb der Risikokultur als Leitplanken.

These 10: Eine starke Risikokultur stellt eine Gemeinschaftsarbeit dar, sie funktioniert nicht als Leistung eines Einzelnen.

2.1 DEFINITION DER RISIKOKULTUR

Lediglich ein Institut konnte keine ausformulierte Definition für Risikokultur aufweisen, plant dies jedoch im kommenden Jahr zu ändern – alle anderen Institute nutzen eine eindeutige Definition, häufig verortet in einer „Leitlinie Risikokultur" (40 %) oder im Risikoappetit/der Risikostrategie (30 %).

In großer Mehrheit behandelt die gewählte Definition der Risikokultur sowohl finanzielle als auch nicht-finanzielle Risiken (>95 %) und unterstreicht somit eine übergreifende Relevanz für alle Bereiche. Daraus abgeleitet ist die Risikokulturdefinition bei einigen Instituten (20 %) auch in mehreren Leitlinien verankert. Weitere genannte Kernelemente sind Normen, Einstellungen und Verhaltensweisen entsprechend den Guidelines on Internal Governance der EBA. Daher ist die häufigste Referenz, die für die Risikokulturdefinition verwendet wird, die der EBA (40 %), gefolgt von anderen einschlägigen Definitionen des Basel Komitees, des FSB, der MaRisk und der BaFin. Nur ein Viertel der Institute nennt keine regulatorische Referenz für die eigene Risikokulturdefinition.

Bei mehr als der Hälfte der Institute wird das enge Zusammenspiel von Unternehmens- und Risikokultur herausgestellt und die Risikokultur als tragende Säule der Unternehmenskultur beschrieben. Dabei verdeutlichen die Teilnehmer, dass die Unternehmenskultur selten losgelöst von der Risikokultur bestehen kann und die Einstellung von Führungskräfte und Mitarbeitenden zu Risikokultur, -bewusstsein und -bereitschaft direkt mit der gelebten Unternehmenskultur zusammenhängt. Sieben der Institute sehen Risikokultur als Teil der Unternehmenskultur, weitere sechs als direkt aus ihr abgeleitet. Lediglich zwei Banken sehen keinen direkten Bezug. Unsere These 2, *„die Risikokultur ist in die Organisationskultur eines Unternehmens eingebettet. Die Fehlerkultur ist dabei ein Teilelement der Risikokultur, Compliance- und Risikokultur überlappen sich"* findet damit eine klare Bestätigung durch die befragten Institute – zumindest eine gelebte Fehlerkultur kann jedes Institut vorweisen

2.2 OPERATIVE VERANTWORTLICHKEITEN IM RISIKOKULTUR-KONTEXT

Neben der Risikokultur selbst sollten auch die dafür bestehenden Verantwortlichkeiten klar definiert sein. Als operativ verantwortlich werden am häufigsten verschiedene Risikoabteilungen genannt, die am ehesten für Definition (50 %), Dokumentation (60 %), Messung (50 %) und Kommunikation/Reporting (50 %) der Risikokultur zuständig seien. Bei 20 % der Institute ist der Bereich Compliance für die Weiterentwicklung der Risikokultur (mit-) verantwortlich. Sofern die Aufgaben von Definition bis Reporting nicht zentral in den Bereichen Risiko oder Compliance liegen, sehen die Institute die individuelle Verantwortung in den jeweiligen Fachbereichen. Die Verantwortung für die eng mit der Risikokultur verwobene Unternehmenskultur liegt jedoch meist bei der Geschäftsleitung und dem Geschäftsleitungsstab (60%); hier sehen nur 16% der Institute die Risikofunktion in der Pflicht und weitere 20% sehen die Verantwortung für die Weiterentwicklung der Unternehmenskultur in der Personalabteilung.

Innerhalb der Risikofunktion zeigt sich ein heterogenes Bild mit etwa gleich verteilten Antworten – sie verankern die Verantwortung jeweils in den Bereichen Enterprise Risk Management (ERM), Non-Financial Risk (NFR) und operativem Risikomanagement oder bei der allgemeinen Risikofunktion. Einig sind sich die teilnehmenden Institute darin, dass gerade die Definition der Risikokultur in enger Abstimmung mit der Führungsebene geschehen muss und unterstreichen somit erneut die enge Verknüpfung von Unternehmens- und Risikokultur (50 %). Stärker operativ geprägte Aufgaben wie Messung, Kommunikation und Reporting finden sich häufig als Gemeinschaftsverantwortung über ERM, NFR und operatives Risikomanagement verteilt – betont wird hier die koordinative Rolle der Risikofunktion, die sich auf die Einzelverantwortung im Fachbereich und enge Abstimmung mit der Führungsebene stützt.

Auf Geschäftsleitungsebene nimmt der CRO eine zentrale Rolle ein – auch bei der Aufgabe, die Eigenverantwortung bei den Mitarbeitenden zu festigen – und ist folglich ein primärer Stakeholder der Risikokultur: Bei 70 % der Banken ist der CRO hauptverantwortlich für die Risikokultur; zwei Drittel bezeichnen ihn als maßgeblich für den wichtigen „Tone from the Top"; und die Hälfte unterstreicht dessen Verantwortung für Definition und Kommunikation der Risikokultur und gibt an, dass die übrigen Geschäftsleitungsmitglieder die Definition der Risikokul-

tur unterstützen und diese durch aktive Förderung und Überwachung begleiten. Währenddessen wird der Aufsichtsrat von den meisten Banken (80 %) als primäre Überwachungsinstanz angesehen und nur bei 20 % der Banken ist die Rolle des Aufsichtsrats als Stakeholder der Risikokultur nicht explizit definiert. Weitere Stakeholder der Risikokultur sind die Mitarbeitenden mit ihrer Eigenverantwortung für die Aufrechterhaltung und gelebte Praxis der Risikokultur sowie die 3rd Line of Defense (3LOD) als zusätzlich prüfende Instanz. Diese breite Verteilung der Stakeholder betont weiterhin die übergreifende Relevanz von Risikokultur, beginnend bei CRO, Geschäftsleitung und Aufsichtsrat bis hin zur Verantwortung aller Mitarbeitenden über alle Bereiche hinweg. Die These 1, *„Risikokultur manifestiert sich in verschiedenen Elementen einer Organisation, beispielsweise in Chance-Risiko-Abwägungen bei Entscheidungen"* lässt sich jedoch nur teilweise bestätigen, da aus der Befragung nicht klar hervorgeht, wie viele Institute tatsächlich Chance-Risiko-Abwägungen standardisiert in Entscheidungsprozessen verankert haben.

2.3 BEWERTUNG, REPORTING UND KOMMUNIKATION DER RISIKOKULTUR

Für eine funktionierende Risikokultur bedarf es nicht nur klar definierter, operativer Verantwortlichkeiten, sondern auch einer kontinuierlichen Messung, eines aussagefähigen Reportings und effektiver Kommunikation.

Im Kern der Risikokulturmessung steht die Identifikation potenzieller Schwächen und Verbesserungspotenziale für die Risikokultur – in 90 % der Institute findet eine solche Prüfung und Messung regelmäßig statt, in der Hälfte der Banken jährlich. Am häufigsten werden Umfragen für eine solche Messung genutzt, teilweise integriert in andere Mitarbeiterbefragungen (40 %), häufiger aber in dedizierten Risikokulturumfragen (60 %), die typischerweise ca. 20 Fragen umfassen. Externe Industrievergleiche oder ein Vergleich mit anderen Banken werden eher selten eingesetzt (30 %) – und wenn, dann mit externen Dienstleistern erstellt.

Für ein granulares Reporting fehlt in den meisten Fällen ein messbares Zielbild, denn nur ein Viertel der Banken erhebt quantifizierbare Kennzahlen; häufiger werden nur Verstöße erfasst. Somit haben auch nur 40 % der teilnehmenden Institute ein KPI-basiertes Reporting, das in zwei Dritteln dieser Banken jährlich durchgeführt wird und hauptsächlich auf Umfragen und anderen NFR-Metriken basiert. Meist ist dieses Reporting in das generelle NFR-Reporting integriert.

Die Kommunikation der Risikokultur geschieht in den Instituten mehrheitlich (70 %) durch konkrete, prinzipienorientierte Leitlinien, die den Mitarbeitenden bekannt gemacht werden und sich häufig deckungsgleich im Code of Conduct wiederfinden. Die Formalisierung als Handlungsrichtlinie bestätigt damit auch unsere These 4, dass es *„einer Balance zwischen Formalisierung und Freiheitsgraden bedarf, um die Entscheidungsfähigkeit des Einzelnen sicherzustellen"*.

Eine Kommunikation durch Verankerung in Ziel- und/oder Vergütungsvereinbarungen gibt es nahezu nicht (10%) – die überwiegend genannte Kommunikationsmethodik ist der „Tone from the Top", d. h. die Kommunikation, aber auch das Vorleben durch die Führungsebene und insbesondere die Geschäftsleitung. Die befragten Banken nennen hier klar eine Chance in der bereichsübergreifenden Kommunikation, um über Schnittstellen hinweg Klarheit zu schaffen und die Bedeutung der Risikokultur zu unterstreichen. In Kombination mit Leitlinien, Code of Conduct sowie Handlungsempfehlungen und Trainings seitens der Personalabteilung bildet dies die Kommunikation der Risikokultur im Teilnehmerfeld ab. Herauszustellen ist dabei, dass Transparenz gegenüber Mitarbeitern sowie ein offener Diskurs die Glaubwürdigkeit der Führungsebene untermauert, die Risikokultur stärkt und ein gemeinschaftliches Verständnis und Bewusstsein schafft.

Gemeinschaftsverantwortung als zentrales Element für Risikokultur belegt unsere These 10, dass *„eine starke Risikokultur eine Gemeinschaftsarbeit darstellt und nicht als Leistung eines Einzelnen funktioniert"*. Die von den Instituten überwiegend unterstrichene Vorbildfunktion der Führungsebene und Verantwortung einer bzw. eines jeden einzelnen Mitarbeitenden bestätigt zudem auch These 5, da *„die Kongruenz von Wort und Tat von allen im Unternehmen ein wesentliches Element einer robusten Risikokultur darstellt."*

2.4 STÄRKEN UND SCHWÄCHEN BEI DER AUSGESTALTUNG DER RISIKOKULTUR

Zusätzlich zu Fragen zur Definition und operativen Handhabung wurden die teilnehmenden Banken um eine Bewertung der momentanen Ausgestaltung der Risikokultur gebeten. Dazu wurden einzelne Stärken und Schwächen in der Selbstwahrnehmung der Banken abgefragt, zudem beurteilten die befragten Führungskräfte die Effektivität einzelner Ausgestaltungsmaßnahmen.

Insgesamt zeigen sich in der Eigenwahrnehmung Stärken hauptsächlich in der Konzeptionierung der Risikokultur, denn vor allem die Definition, die Risikostrategie und der Risikoappetit werden von den Instituten als Stärken identifiziert. Hinzu kommen eine bereichsübergreifende Umsetzung und eine konstruktive Fehlerkultur, die ebenfalls in mehreren Banken als eigene Stärken gelten. Dies bestätigt unsere These 8 zum *„Akzeptieren von Fehlern, das Lernen aus Fehlern sowie das Feedback des Gelernten zurück in die Organisation zur Förderung einer starken Risikokultur"*, denn offenbar setzen die Institute klare Prioritäten

auf Fehlerkultur und Rückkopplungsprozesse und sehen darin auch eigene Stärken.

In der konkreten operativen Einbindung der Risikokultur sehen die befragten Institute aber auch Schwachstellen. Gerade in bereichsübergreifenden Prozessen wird in einigen Instituten eine gelebte Risikokultur noch vermisst. Eine gewisse Ambivalenz ergibt sich in der bereichsübergreifenden Umsetzung, da zwar mehrere Institute dies als eine ihrer Stärken definieren, ebenso viele aber eine eigene Schwäche bei der Umsetzung über Schnittstellen hinweg erkennen. Darüber hinaus werden der „Tone from the Top", die allgemeine Kommunikation und die Dokumentation der Risikokultur als Schwächen identifiziert. Somit findet sich zwar eine überwiegende Bestätigung des Konzepts von These 3, dass *„eine durchlässige Organisationsstruktur, funktionierende Prozesse, fest verankerte Werte sowie das angemessene Verhalten des Einzelnen die Grundfeste einer robusten Risikokultur bilden*," jedoch mit Verbesserungspotenzial für bereichsübergreifende Prozesse. Die These 6, die *„eine klare und leicht verständliche Sprache (innerhalb der Organisation und auch als Tone from the Top), eindeutig formulierte Erwartungen sowie die Konsistenz der gesendeten Botschaften über Zeit*" als wichtige Unterstützung für Risikokultur-Kommunikation nennt, findet ebenso in den befragten Instituten als zentraler Bestandteil für effektive Kommunikation Bestätigung.

Maßnahmen zur Ausgestaltung und Weiterentwicklung der Risikokultur sowie zur Behebung der gefundenen Schwächen finden sich in Form von gezielten Programmen und anderen Aktivitäten bei zwei Dritteln der Institute wieder. Sie sprechen sich für Kommunikationsmaßnahmen, Trainings und Rückkopplungsprozesse als effektive Gestaltungsmaßnahmen aus. Dabei ist insbesondere die glaubhafte Einbindung der Führungsebene und der Geschäftsleitung von Bedeutung, ebenso wie die Nutzung neuer Trainingsformate (z.B. Videoseminare). Weniger bedeutsam sind nach Aussage der Befragten monetäre Anreize, aber auch Sanktionen – die Institute bestätigen somit wenig bis gar nicht unsere These 9, dass *„angemessene Sanktionen und Konsequenzen innerhalb der Risikokultur als Leitplanken fungieren*." Lediglich teilweise ließ sich These 7 untermauern, dass sich *„über gezielte Anreize (nicht nur monetärer Art) und Interventionen die Risikokultur immer wieder in das Bewusstsein des Einzelnen holen sowie gezielt stärken lässt*", denn eine Integration ins Vergütungssystem wurde selten bis gar nicht als Zukunftsperspektive genannt und auch Interventionen wurden kaum von den Instituten thematisiert.

3. AUSBLICK: POSITIVE EINFLÜSSE EINER ROBUSTEN RISIKOKULTUR BEI DER KRISENBEWÄLTIGUNG

Das Management nicht-finanzieller Risiken ist während einer Pandemie von zentraler Bedeutung, wie wir in den Jahren 2020 und 2021 gesehen haben. In dieser Hinsicht wirkt die Covid-19-Pandemie wie ein realer Stresstest, auf den sich die Organisation kaum vorbereiten kann. Der Russland/Ukraine-Konflikt und andere Krisen (oft mit Bezug zu ESG-Themen) stellen Banken und andere Finanzinstitute vor weitere Herausforderungen, die meist eine unverzügliche Anpassung der Prozesse erfordern.

Viele Banken haben in den vergangenen Jahren diese besonderen Herausforderungen erfolgreich gemeistert. Ein Grund dafür könnte das antrainierte Verhaltensmuster für die Zusammenarbeit in der Organisation sein, also die Unternehmens- und speziell die Risikokultur, in der jeder Einzelne antizipieren kann, was zu tun und zu lassen ist, ohne dass dies in Richtlinien detailliert beschrieben wird und ohne ein für diese spezielle Situation konzipiertes internes Kontrollsystem.[6]

Das koordinierte Zusammenwirken aller für das Risikomanagement zuständigen Stellen ist integraler Bestandteil einer positiven Risikokultur. Ähnlich wie in einem Theaterstück, in dem jeder seine Rolle kennt, findet in diesem Rahmen eine „Choreografie des Risikomanagements" für unvorhersehbare Situationen auf der Grundlage einer Art von Risikowertekanon statt. Teil der Risikokultur ist das tägliche Training von Rollen und Verantwortlichkeiten, damit sie auch in Krisensituationen funktionieren.

Die oberste Leitungsebene gibt den Rahmen für das Verhalten im Umgang mit Risiken vor und definiert den Handlungsspielraum; diesen Rahmen gilt es so belastbar wie möglich zu machen. Hierzu gehört, dass die Risikofaktoren adäquat überwacht werden und die Organisation in die Lage versetzt wird, auf Unvorhergesehenes und Krisen angemessen zu reagieren. Wenn also beispielsweise zu Beginn der Pandemie die Unternehmensleitung bei ihren Entscheidungen zur Reduzierung der NFR keinen Zweifel daran gelassen hat, dass die Gesundheit der Mitarbeitenden oberste Priorität hat und dass jegliche Risiken in dieser Hinsicht bestmöglich ausgeschlossen werden sollten, ist dies ein Ausdruck der Risikokultur und der Risikobereitschaft. Die Bereitschaft der Unternehmensleitung zu hohen Investitionen in das technische Umfeld, um mobiles Arbeiten zu ermöglichen, kann auch für die kulturellen Werte des Unternehmens – nicht zuletzt für die Risikokultur – stehen, im Sinne eines positiven „Tone from the Top".

Im Kontext von Covid-19 ist das Wertesystem, das unter anderem die Unternehmens- und die Risikokultur einschließt, noch wichtiger geworden. Das digitale Kollaborationsmodell könnte das bestehende und u.a. auf Unterschriftenkontrollen und Händlerüberwachung basierende Kontrollsystem für zahlreiche Risiken anfälliger machen. Sollen Risiken und finanzielle Verluste vermieden werden, so sind die Wachsamkeit und Verantwortung jedes Einzelnen in jeder Verteidigungslinie deutlich mehr gefordert. Die entscheidende Frage ist, ob die verschiedenen Möglichkeiten, mittels passgenauer Interventionen Verantwortung und Rechenschaftspflicht in den Köpfen der Mitarbeiter

6 Diese und die weiteren Ausführungen in Kapitel 3 basieren auf dem Artikel von Schmidt, Bodo/ Scheibel, Thorsten (2021), "It's the culture, stupid": Risk culture as the key building block of NFR management – and why some banks have come through the Covid-19 pandemic better than others

(und nicht allein in formellen Regeln und Richtlinien) zu verankern und dadurch die Risikokultur zu stärken, ausreichend genutzt werden.[7]

Dies gilt umso mehr, als im Hinblick auf die Zusammenarbeit oft vom „Beziehungskapital" die Rede ist, das in der virtuellen Welt zu schwinden drohe. Dies betrifft etwa die zufälligen Treffen von Kolleg:innen an der Kaffeemaschine oder auf dem Weg zur Kantine, die so genannten Impulsbegegnungen. Die bei solchen Gelegenheiten stattfindenden spontanen Gespräche liefern wertvolle Denkanstöße zur Überwindung von Hürden, die zwangsläufig in einer Aufbauorganisaiton vorhanden sind. In der Zeit der Pandemie mit Homeoffice und vielfach leeren Büros sind solche informellen Kontakte weitgehend entfallen, man ist einander „fremd geworden". Die mögliche Folge: eine Schwächung von Vertrauen und Risikokultur.

Zugleich erlangte in der neuen, vorwiegend digitalen Umgebung die erste Verteidigungslinie eine viel größere Bedeutung im Hinblick auf das Risikomanagement. Bestehende Kontrollen mussten so weit wie möglich angepasst und neue, wirksame Kontrollen eingeführt werden. Bis das neue Kontrollumfeld geschaffen war, gingen die Geschäftsleitungen Risiken ein, die sie zu dem Zeitpunkt noch nicht vollständig überblicken und valide einschätzen konnten. In der neuen digitalen Umgebung ist ein vollständiger Schutz gegen diese Risiken durch Kontrollen vermutlich nicht realisierbar. Umso wichtiger waren und sind die Menschen im Unternehmen: Sie erhielten mehr Verantwortung für ihr Verhalten und mehr „Eigenkontrolle" – auch ohne dass dies in Richtlinien für die neue Arbeitssituation verankert wurde.

Traditionell denken und handeln Banken mit ausgeprägter Langfristperspektive, und lange Zeit geschah dies in einem – im Vergleich mit der aktuellen Lage – eher stabilen und im wörtlichen Sinn berechenbaren Umfeld. Doch je volatiler die Rahmenbedingungen des Geschäfts werden, desto wichtiger ist eine robuste Risikokultur – sie ist ein Schlüssel zur Bewältigung akuter Krisen und zur Entwicklung von Resilienz. Dies spiegelt sich in der jüngst verstärkten aufsichtlichen Aktivität zum Thema Risikokultur wider und zeigt sich auch in den Ergebnissen der FIRM-Befragung.

Nach der Krise ist vor der Krise. Viele Banken sind im „Stresstest" der Pandemie widerstandsfähiger gegen unerwartete Umstände geworden – jetzt gilt es die richtigen Schlüsse aus der bislang erfolgreichen Bewältigung der Pandemie zu ziehen, um auf die nächste Krise (bei der es sich nicht um eine Pandemie handeln muss, wie uns die aktuelle geopolitische Lage verdeutlicht) noch besser vorbereitet zu sein.

FIRM und alle im Arbeitskreis „Risikokultur" mitwirkenden Mitglieder bedanken sich herzlich bei den befragten Banken und ihren Verantwortlichen für die Teilnahme an der Umfrage und für die Bereitstellung wertvoller Einblicke in die Ausgestaltung der Risikokultur.

LITERATUR- UND QUELLENVERZEICHNIS

BaFin (2022), BaFin – Konsultation 06/2022 – Entwurf der MaRisk vom 26.09.2022

BaFin (2021), BaFin – Rundschreiben – Rundschreiben 10/2021 (BA) - MaRisk BA

BCBS (2015), Corporate governance principles for banks (bis.org)

EBA (2021): Leitlinien zur internen Governance, EBA/GL/2021/05

ECB (2016), SSM supervisory statement on governance and risk appetite

EU-Eigenkapitalrichtlinie (2013)

Financial Stability Board (2016), Guidance on Supervisory Interaction with Financial Institutions on Risk Culture: A Framework for Assessing Risk Culture (fsb.org)

Financial Stability Board (2017), Stocktake of efforts to strengthen governance frameworks to mitigate misconduct risks

Financial Stability Board (2018), Strengthening Governance Frameworks to Mitigate Misconduct Risk: A Toolkit for Firms and Supervisors (fsb.org)

G30 (2018), Banking Conduct and Culture

Higgins R, Liou G, Maurenbrecher S, Poppensieker T, White O (2021), „Strengthening institutional risk and integrity culture", McKinsey & Company, 2. November 2020; https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/strengthening-institutional-risk-and-integrity-culture

IDW (2022), IDW PS 340 n.F. 01.2022

Schmidt B, Scheibel T (2021), "It's the culture, stupid": Risk culture as the key building block of NFR management – and why some banks have come through the Covid-19 pandemic better than others in: Thomas Kaiser (Hrsg.), Non-Financial Risk Management: Emerging stronger after Covid-19, Risk Books, London 2021

Wirtschaftprüferhandbuch (2020).

7 Für weitere Einzelheiten in diesem Zusammenhang, siehe: Higgins R, Liou G, Maurenbrecher S, Poppensieker T, White O (2020), „Strengthening institutional risk and integrity culture"