Riediger (Hrsg.)

MaRisk-Berichtswesen

Aufsichtliche Vorgaben ● Datenqualität ● Risikosteuerung & -überwachung ● Informationstechnologie ● Auslagerungen ● Compliance ● Aufsichtsrat

FCH AG, 2024

Riediger (Hrsg.)

MaRisk-Berichtswesen

Aufsichtliche Vorgaben • Datenqualität • Risikosteuerung & -überwachung • Informationstechnologie • Auslagerungen • Compliance • Aufsichtsrat

Christian Bachert
Executive Partner Business Consulting
Bereich Finance & Capital Markets
msg for banking ag

Kevin Dominique Bröde
Nachhaltigkeitsmanager Vorstandsstab
Förde Sparkasse

Annika Eberwein
Risikocontrollerin Controlling
Kasseler Sparkasse

Michael Gastmann
Auslagerungs- & Datenschutzbeauftragter
Stabsstelle Überwachungsmanagement
Volksbank im Münsterland eG

Dr. Stephan Genzel
Fachreferent IT-Governance und Sicherheit
Stadtsparkasse München

Prof. Dr. Matthias Haug
Vorstandsmitglied
Volksbank Flein-Talheim eG

Barbara Hugo-Dilworth
Zentrale Auslagerungsbeauftragte Strategie
IKB Deutsche Industriebank AG

Dr. Frank Leitner
Leiter Interne Revision
Daimler Truck AG

Oliver Michelmann
Fachprüfer im Referat Bankgeschäftliche Prüfungen
Deutsche Bundesbank Hannover

Dr. David Miersch
Senior-Referent Validierung
Sparkasse KölnBonn

Markus Müller
Deputy Head MaRisk Compliance, Vice President
Citigroup Global Markets Europe AG Frankfurt/Main

Philipp Plumanns
Spezialist Risikomanagement
AWADO GmbH Wirtschaftsprüfungsgesellschaft
Steuerberatungsgesellschaft Neu-Isenburg

Simone Richter
Stellv. Compliance-Beauftragte
Helaba Invest Kapitalanlagegesellschaft mbH

Henning Riediger (Hrsg.)
Prüfungsleiter im Referat Bankgeschäftliche Prüfungen
Deutsche Bundesbank Hannover

Dr. Normen Rohde
Risikocontrolling
Berliner Volksbank eG

René Schilling
Experte Risikomanagement Unternehmenssteuerung
Stadt- und Kreissparkasse Leipzig

Lars Schleifer
Meldewesen
Volksbank Mittelhessen eG

Dennis Schulte
Freiberuflicher Autor und Mitarbeiter im Gesamtbankcontrolling
Sparkasse Osnabrück

Ron Schwach
Senior Business Consultant
Capital & Financial Management
msg for banking ag

Dr. Gennadij Seel
Direktor Gesamtbanksteuerung & Spezialkredite
Sparkasse Düren
Dozent an der FOM sowie Research Fellows
Institute for Strategic Finance

Daniel Storch
Spezialist Gesamtbanksteuerung und Risikomanagement
Umweltbank AG

FCH AG, 2024

Inhaltsübersicht

Inhaltsverzeichnis

A.

Einleitung, Zweck und Aufbau des Werkes

A. Einleitung, Zweck und Aufbau des Werkes[1]

I. Einleitung und strukturierter Themenüberblick

Inwiefern unterscheiden sich eigentlich das moderne Fliegen eines Flugzeugs und das Führen eines Kreditinstituts? 1

Zunächst wird man relativ viele Gemeinsamkeiten feststellen können: 2

- Der Pilot hat ein Ziel, welches er anfliegt und weiß, wie er dort hinkommen möchte. Der Vorstand hat ein Geschäftsmodell und daraus bestimmte Ziele abgeleitet und weiß, wie man sie erreichen will.
- Der Pilot verlässt sich auf die Instrumente und Anzeigen und kann mit seiner »originären« Sicht die Flugroute plausibilisieren. Der Vorstand verlässt sich auf die erhaltenen Informationen aus Berichten und plausibilisiert die Entwicklung an der Zielerreichung.
- Der Pilot muss auf ausreichend Höhe bzw. Auftrieb achten und dabei immer die Treibstoffreserven im Blick haben. Der Vorstand muss auf ausreichende Solvabilität achten und immer die Liquidität im Blick haben.
- Die Anzeigetafeln im Cockpit weisen den Piloten auf mögliche Probleme und Fehlentwicklungen hin. Im Institut müssen Frühwarnindikatoren und Warnschwellen eingerichtet werden, welche dem Vorstand rechtzeitig die notwendigen Impulse geben.
- Sowohl der Flugbetrieb als auch Institute unterliegen einer Aufsicht.

Neben diesen vielen Gemeinsamkeiten besteht jedoch ein wesentlicher Unterschied: **In einem Kreditinstitut gibt es keinen Autopiloten!** 3

Dieser wesentliche Unterschied begründet zudem, dass das Risikomanagement eines Instituts permanent erfolgen muss. Ausruhen und »fliegen lassen« gibt es demnach nicht. Es ist also der fortlaufende Prozess des Steuerns und Überwachens, welcher den Erfolg des Instituts sicherstellt. 4

Nun soll dieses Buch keinen Einblick in die Höhen der Luftfahrt, sondern in die Tiefen des Berichtswesens bzw. des Reportings geben. Oder einfacher ausgedrückt, sollen die folgenden Fragen beantwortet werden: 5

- Auf welche Anzeigen ist zu achten?
- Wie sollten die Anzeigen kalibriert werden?

1 Autor: **Henning Riediger**. Die Ausführungen geben die persönliche Auffassung des Autors wieder, die nicht notwendigerweise mit der der Deutschen Bundesbank übereinstimmen muss.

- Welche Interpretationsmöglichkeiten gibt es?
- Welche Maßnahmen sind abzuleiten und umzusetzen?
- Was sind kritische Anzeigekombinationen?
- Wie oft muss auf die Anzeigen geschaut werden?

6 Somit sind wir also mittendrin in den wesentlichen Fragestellungen und Aspekten des Berichtswesens. Der Fokus des vorliegenden Werkes richtet sich sowohl auf die Vorgehensweisen der Auftraggeber und der Ersteller als auch auf die sich anschließenden Handlungen der Empfänger von Berichten.

7 Bereits im Jahr 2018 wurde mit dem Herausgeberwerk »Risikoreporting«[2] vom Herausgeber und Autor eine identische Einleitung in das Thema gewählt, denn das Thema ist nach wie vor von hoher Praxisrelevanz. Der Herausgeber und der Verlag haben sich daher entschieden, das Thema in einem neuen Format aufzugreifen und den Fokus deutlich stärker als 2018 auf die MaRisk-bezogenen berichtsrelevanten Themen zu legen. Bewusst wurden wieder Autoren aus Aufsicht, Praxis, Beratung und Prüfung einbezogen, um durch die Kombination der Autoren einen erheblichen Mehrwert zu schaffen. Der Fokus der aus der Aufsicht stammenden Autoren richtet sich auf Erfahrungen aus der Prüfungspraxis und stellt dabei auf wiederholt auftretende Probleme in Bezug auf Vollständigkeit und Konsistenz der Methoden im Risikomanagement ab. Die Passagen der Institutspraktiker stellen verschiedene Lösungsansätze aus den Instituten sowie unterstützende Berichtslösungen vor und zeigen die Chancen und ebenso die Risiken der jeweiligen Vorgehensweisen auf.

8 Beginnend im folgenden Abschnitt B werden die Grundzüge und erforderlichen Ausgestaltungsmerkmale eines angemessenen Berichtswesens dargestellt und erörtert. Nachfolgend wird auf die Verknüpfung mit den strategischen Vorgaben als Sollgeber für das Berichtswesen sowie die Datenqualität abgestellt.

9 Auf dieses Grundlagen-Kapitel folgt das Kapitel C, welches sich auf das institutsinterne Berichtswesen in ausgewählten risikorelevanten Bereichen eines Kreditinstituts fokussiert. Hierzu wurden aus aktuellen Anlässen der Schwerpunkt auf die Neuerungen bei der Überprüfung der Risikotragfähigkeit, die Berichterstattung zu ESG-Risiken sowie von bzw. über Auslagerungsunternehmen gelegt.

2 Vgl. *Riediger, H.* (2018a), Abschnitt A.

Die Berichterstattung über die Situation des Instituts endet bekanntlich nicht bei der Geschäftsleitung, sondern schließt das Aufsichtsorgan mit ein. Insbesondere die rechtzeitige und vollständige Information des Aufsichtsorgans ist nach Einschätzung des Herausgebers so zentral, dass dieses Thema mit dem Kapitel D gezielt »vor die Klammer« gezogen wurde. 10

Die vorgenannte Klammer bildet das Kapitel E mit den Beiträgen der Praktiker aus den Instituten. Die Themen wurden anhand der Erfahrungen des Herausgebers mit den Inhalten der MaRisk ausgewählt. Schwerpunkt bilden auch hier zunächst die Berichtsformate aus dem Umfeld des ICAAP: normative und ökonomische Perspektiven bei der Überprüfung der Risikotragfähigkeit, Stresstests, Validierung der eingesetzten Verfahren sowie als herausgehobenes Thema die Berichterstattung zu den Adressrisiken. Anschließend stehen die Operationellen Risiken aus dem Einsatz der Informationstechnologie sowie aus Auslagerungen im Fokus. Nachfolgend werden die Themen Compliance und ESG-Risiken intensiv behandelt. Gerade diese beiden Themen werden zukünftig von Anpassungen der aufsichtlichen Benchmark betroffen sein, so dass eine frühzeitige und angemessene Auseinandersetzung geboten sein dürfte. Den Abschluss dieses Klammer-Kapitels stellt die Befassung mit berichtsrelevanten Inhalten aus dem Umfeld der Liquidität dar. Es werden gezielt Hinweise gegeben, wie bereits aus dem Umfeld aufsichtlicher Meldungen systematisch Synergien für die interne Steuerung geschaffen werden können. 11

Besonderen Fokus wurde somit bei der Auswahl der Themen auf die verschiedenen **Funktionseinheiten** in Kreditinstituten gelegt. Diese Abschnitte umfassen die Themen der besonderen Funktionen sowohl des Risikocontrolling-, des Compliance- sowie des IT-Sicherheitsbeauftragten. Diese Berichtskanäle sind für ein angemessenes Risikomanagement bzw. für die Steuerung des Instituts in der Praxis nicht zu unterschätzen und daher gezielt praxisorientiert. 12

Im Kapitel F werden beispielhafte Berichtslösungen und -formate vorgestellt, welche insbesondere bei der Ableitung der notwendigen Steuerungsimpulse und Handlungsmaßnahmen unterstützend wirken können. 13

Den Abschluss des Gesamtwerkes im Kapitel G bildet die Schwerpunktsetzung der Prüfung des Berichtswesens seitens der internen und externen Revision. Hier liefern die Autoren wertvolle Hinweise und Anregungen, um die Wirksamkeit des Internen Kontrollsystems in angemessener Art und Weise zu überprüfen. 14

Es sei noch hinzugefügt, dass es sich in vielen Fällen um die persönlichen Auffassungen der Autoren handelt und nicht zwingend mit denen des jeweiligen 15

Dienstherrn bzw. Arbeitgebers übereinstimmen müssen. Zudem bitten ich als Herausgeber immer zu prüfen, inwiefern und unter welchen Maßgaben die in diesem Werk dargestellten Vorgehensweisen im Berichtswesen für das eigene Institut des Lesenden als tatsächlich angemessen einzustufen sind. Das Ziel ist es daher nicht, bestimmte Lösungen vorzuschreiben, sondern zur Diskussion im Institut, zwischen Instituten sowie insbesondere zwischen Institut und Dienstleistern anzuregen. In diesem Sinne wünsche ich Ihnen beim Lesen viel Spaß und viel Erfolg bei der Bewältigung der vor Ihnen liegenden Aufgaben und Themen.

Henning Riediger

Hannover, 2024

II. MaRisk als Treiber eines angemessenen Berichtswesens

Die fortlaufende Aktualisierung der MaRisk speist sich aus drei verschiedenen Quellen: 16

- Internationale Regulierungsinitiativen,
- Erfahrungen der Bankenaufsicht aus Bankgeschäftlichen Prüfungen und
- Erkenntnisse aus verschiedenen Manipulations- und Betrugsfällen.

Die MaRisk verfolgen einen prinzipienorientierten Ansatz. Dies bedeutet, dass keine detaillierten Einzelfallregelungen und quantitativen Vorgaben enthalten sind. Vor diesem Hintergrund ist auch die Durchführung von Bankgeschäftlichen Prüfungen seitens der Aufsicht kein Prozess des Abhakens von Checklisten, sondern eine institutsindividuelle Würdigung des Risikomanagements bzw. der Geschäftsorganisation. Im Vordergrund steht demnach die Qualität des Risikomanagements, denn den Instituten wird explizit die Eigenverantwortung für die Einrichtung eines angemessenen und wirksamen Risikomanagements eingeräumt bzw. auferlegt. 17

Besondere Bedeutung bei der Anwendung der MaRisk wird dem **Prinzip der doppelten Proportionalität** eingeräumt. Ausgehend von in den MaRisk enthaltenden Mindestanforderungen, müssen in Abhängigkeit von Institutsgröße, Geschäftsumfang, Komplexität der betriebenen Geschäfte und Risikogehalt die Anforderungen steigen, um ein angemessenes Risikomanagement zu gewährleisten. Im direkten Zusammenhang mit der Bedeutung des Instituts für die Finanzmärkte resultiert schlussendlich die Intensivität der aufsichtlichen Überwachung. 18

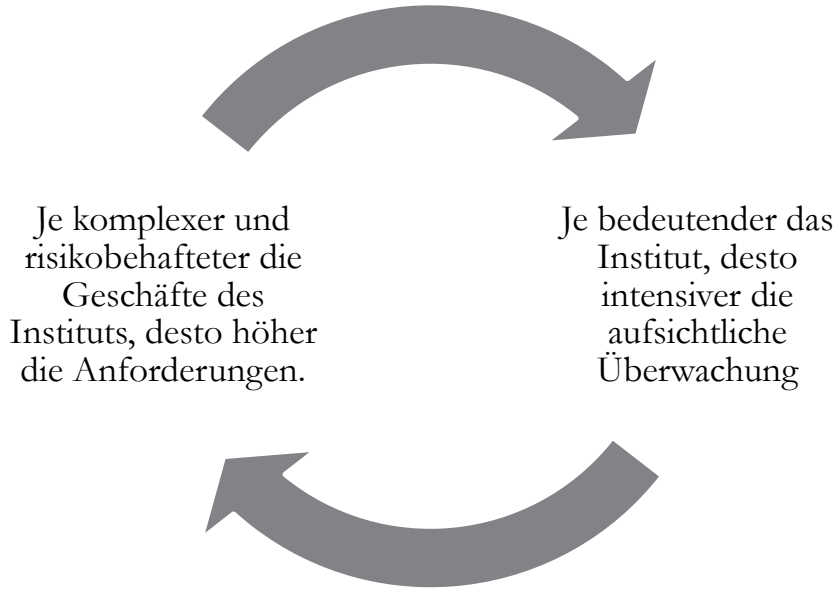

Abbildung A-1: Prinzip der doppelten Proportionalität.[3]

19 Neben den MaRisk sei direkt auf ein weiteres für die Risikosteuerungs- und -überwachungsprozesse wesentliches Dokument verwiesen: den **Leitfaden zur aufsichtlichen Beurteilung bankinterner Risikotragfähigkeitskonzepte** (im Folgenden »RTF-Leitfaden«)[4]. Der Leitfaden basiert auf fünf zentralen Beurteilungsmaßstäben:

(1) das **Proportionalitätsprinzip**, welches die fundamentale Bedeutung der Größe des Instituts sowie der Komplexität der betriebenen Geschäfte für die Ausgestaltung des Konzepts für die Risikotragfähigkeit bzw. -messung betont,

(2) die **Vollständigkeit** der Risikoabbildung aller wesentlichen Risikoarten,

(3) die **Konsistenz** der Verfahren, was ein methodisches Ineinandergreifen von Risikodeckungsmassenermittlung, Limitierung und Risikomessung erfordert,

(4) das **Vorsichtsprinzip**, das die Anwendung ausreichend konservativer Ansätze und Annahmen verlangt und

(5) die **Beurteilung des Einzelfalls** unter Berücksichtigung des Wesentlichkeitsprinzips.

3 Quelle: Eigene Darstellung.
4 Vgl. *BaFin* (2018a).

Eine sprachliche Besonderheit der MaRisk ist der Begriff der **Risikokultur**. Schon die BaFin hat 2015 in ihrer Publikation BaFin-Journal folgende Aussage getroffen: 20

> *»Für die Aufsicht – aber auch für die Institute – ist das Thema Risikokultur zweifellos eines, das sich nur relativ schwer greifen lässt, da es nicht ohne Weiteres isoliert überprüfbar ist.«*[5]

In vielen Gesprächen mit Vertretern der Bankindustrie, mit Kollegen aus der Aufsicht und der Wissenschaft stellte sich der Autor wiederholt die Frage: Worüber reden wir eigentlich? Was fällt unter den Begriff Risikokultur und wie grenzen wir ihn von anderen Begriffen ab. 21

Mit dieser Frage war ich bisher anscheinend auch nicht allein, denn vergleicht man die Definitionen des Begriffs Risikokultur in der folgenden Tabelle, so ergibt sich ein weites Feld an Inhalten und Deutungsmöglichkeiten: 22

Baseler Ausschuss (2015)[6]	Die Normen, Einstellungen und Verhaltensweisen einer Bank in Bezug auf Risikobewusstsein, Risikobereitschaft und Risikomanagement sowie Kontrollen, die Entscheidungen über Risiken beeinflussen. Die Risikokultur beeinflusst die Entscheidungen von Management und Mitarbeitern im Tagesgeschäft und wirkt sich auf die Risiken aus, die sie eingehen.
IRM (2012)[7]	Die Werte, Überzeugungen, Kenntnisse und das Verständnis von Risiken, die von einer Gruppe von Personen mit einem gemeinsamen Zweck geteilt werden, insbesondere von Mitarbeitern einer Organisation oder von Teams oder Gruppen innerhalb einer Organisation.
McKinsey (2010)[8]	Die Verhaltensnormen für Einzelpersonen und Gruppen innerhalb einer Organisation, die die kollektive Fähigkeit bestimmen, die gegenwärtigen und zukünftigen Risiken der Organisation zu identifizieren, zu verstehen, offen zu diskutieren und darauf zu reagieren.
BaFin (2023)[9]	Die Risikokultur beschreibt allgemein die Art und Weise, wie Mitarbeiter des Instituts im Rahmen ihrer Tätigkeit mit Risiken umgehen (sollen). Die Risikokultur soll die Identifizierung und den bewussten Umgang mit

5 Vgl. *BaFin* (2015), S. 23.
6 Vgl. *BCBS* (2015), S. 5.
7 Vgl. *Institute of Riskmanagement* (2012), S. 7.
8 Vgl. *Levy, C./Lamarre, E./Twining, J.* (2010), S. 3.
9 Vgl. *BaFin* (2023), AT 3 Tz. 1 MaRisk.

	Risiken fördern und sicherstellen, dass Entscheidungsprozesse zu Ergebnissen führen, die auch unter Risikogesichtspunkten ausgewogen sind. Kennzeichnend für eine angemessene Risikokultur ist vor allem das klare Bekenntnis der Geschäftsleitung zu risikoangemessenem Verhalten, die strikte Beachtung des durch die Geschäftsleitung kommunizierten Risikoappetits durch alle Mitarbeiter und die Ermöglichung und Förderung eines transparenten und offenen Dialogs innerhalb des Instituts zu risikorelevanten Fragen.

Tabelle A-1: Unterschiedliche Interpretationen zur Risikokultur.[10]

23 Es zeigen sich hierbei deutliche Gemeinsamkeiten beim Adressatenkreis. So werden nicht nur einzelne ausgewählte Funktionen (z. B. der Vorstand, Beauftragte oder Revision) angesprochen, sondern im Prinzip sämtliche Funktionsträger einer Organisation (z. B. eines Instituts). Im Aufsichts-Deutsch spricht man an dieser Stelle von einem »ganzheitlichen Blick«. Nicht ganz so eindeutig sind die Begriffsbestimmungen im Hinblick auf die einzubeziehenden Aspekte. Während beispielsweise beim Baseler Ausschuss (2015) eine enge Orientierung am Risikomanagementprozess erfolgt, werden z. B. bei IRM (2012) weitergehende Aspekte und Maßstäbe wie Werte, Überzeugungen und Kenntnisse einbezogen.

24 Einig sind alle dargestellten Definitionen in Bezug auf die Notwendigkeit der Bewertung einer Risikosituation und die anschließend erforderliche Entscheidung bzw. Maßnahme.

25 Folglich bildet die Risikokultur das Fundament für das Risikomanagement eines Instituts und für Institute ist die Risikokultur damit besonders wichtig, wenn es um die Fragestellung der Angemessenheit der Geschäftsorganisation geht.

26 International ist man sich darüber einig, dass Defizite in der Unternehmensführung bei einer Reihe von Banken dazu beigetragen haben, dass sie in der Vergangenheit unverhältnismäßig hohe Risiken eingingen. Dies hat nicht nur zum Ausfall einzelner Institute, sondern auch durch Rettungspakete jeglicher Art zu einer weiteren Verschärfung kritischer Zustände öffentlicher Haushalte geführt.

27 Zur Vermeidung vergleichbarer Entwicklungen verlangt daher der europäische Gesetzgeber im Erwägungsgrund 54 der Eigenmittelrichtlinie CRD IV, dass die

10 Quelle: Eigene Darstellung in Anlehnung an *Centre for analysis of risk and regulation* (2012), S. 21.

EU-Mitgliedstaaten Grundsätze und Standards einführen, die eine wirksame Kontrolle von Risiken durch die Leitungsorgane von Kreditinstituten und Wertpapierfirmen gewährleisten. Sie sollen, als Teil eines wirksamen Risikomanagements, eine solide Risikokultur auf allen Unternehmensebenen fördern. Da die Eigenmittelrichtlinie CRD kein unmittelbar geltendes Recht darstellt, erfolgte die Umsetzung in diesem Punkt über das Kreditwesengesetz sowie über den AT 3 Tz. 1 MaRisk.

Die Mitglieder der Geschäftsleitung übernehmen immer eine Vorbildfunktion. 28
In ihrem Verhalten soll sich das zuvor von ihnen definierte Wertesystem widerspiegeln, welches die Grundlage für das Verhalten der Mitarbeiter und die Risikokultur bilden soll. Um die angestrebte Risikokultur objektiv überprüfbar zu gestalten hat die Geschäftsleitung gemäß AT 5 Tz. 3g MaRisk einen Verhaltenskodex zu entwickeln, der bestimmt, welches Verhalten akzeptabel ist und welches nicht. Der Verhaltenskodex soll klarstellen, dass die Geschäftsführung von den Mitarbeitern ethisch einwandfreies Verhalten erwartet – dieses dürfte nicht nur durch gesetzliche Vorgaben, sondern in erheblichem Maße auch durch die gesellschaftliche Erwartungshaltung geprägt sein – und illegale Aktivitäten explizit missbilligt. Die Mitglieder der Geschäftsleitung haben ebenso dafür zu sorgen, dass das Wertesystem innerhalb des Instituts kommuniziert, beim Eingehen von Risiken beachtet und mit dem Risikomanagement und den internen Kontrollen verzahnt wird.[11]

Einen thematisch guten Überblick über die relevanten Aspekte, welche bei der 29
Ausgestaltung und Ausprägung der Risikokultur einbezogen werden sollen, gibt die folgende Abbildung:

11 Vgl. *BaFin* (2015), S. 21.

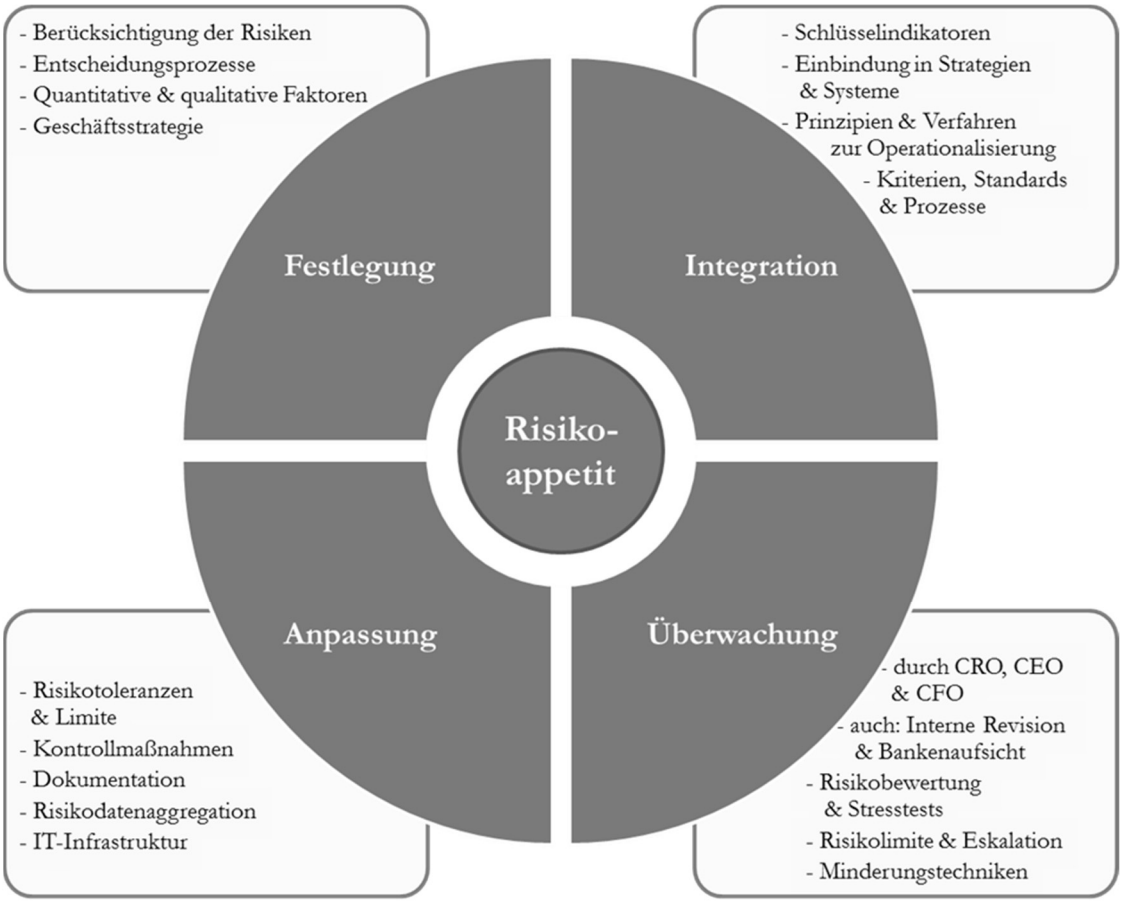

Abbildung A-2: Kernaspekte und Schnittstellen der Risikokultur[12]

30 Zur Umsetzung der Risikokultur bietet sich ein Zitat aus dem BaFin-Journal von August 2015 an:

> *»Um die gewünschte Risikokultur innerhalb eines Unternehmens zu fördern und zu kommunizieren, dessen Beachtung sicherzustellen und unerwünschte Verhaltensweisen zu vermeiden, ist Transparenz und ein möglichst offener Dialog sowohl zwischen Geschäftsleitung und Verwaltungs- beziehungsweise Aufsichtsorgan als auch zwischen Geschäftsleitung beziehungsweise den übrigen leitenden Angestellten und den Mitarbeitern notwendig, und zwar auf sämtlichen Ebenen und zu jedem Zeitpunkt. Alternative Standpunkte, konstruktive Anregungen und Kritik müssen offen kommuniziert werden können (Effective Communication and Challenge). Dazu gehört auch, dass Mitarbeiter vertraulich und ohne Sorge vor Repressalien Bedenken über Praktiken äußern können, die sie für illegal, unethisch oder zumindest fragwürdig halten. Eine angemessene Risikokultur stellt also vor allem eine große Herausforderung an die Führung von Mitarbeitern dar. Sie setzt im Idealfall ein offenes und kollegiales Führungskonzept voraus.«*[13]

12 In Anlehnung an *PricewaterhouseCoopers AG* (2015).
13 Vgl. *BaFin* (2015), S. 22.