

# 05.18

# ZIR

## Zeitschrift Interne Revision

53. Jahrgang  
Oktober 2018  
Seiten 217–272

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

Herausgeber:  
Deutsches Institut für  
Interne Revision e.V.



### Fachzeitschrift für Wissenschaft und Praxis

#### Standards · Regeln · Berufsstand

Prüfung der Risikokultur in Banken 220

*Dr. Christoph Schmidt/Prof. Dr. Svend Reuse*

Implementierungsleitlinien (Teil 2) 232

*Michael Bünis*

#### Management · Best Practice · Arbeitshilfen

Mehrwert von Continuous Auditing 237

*Carsten Jacka/Klaus Persie/Helena Schledewitz/  
Johannes Martin Wagner*

Impairment-Tests 244

*Christoph Wildensee*

#### Wissenschaft · Forschung

Wirtschaftskriminalität und die Interne Revision 253

*Dr. Stefan Hahnenkamp/Dr. Matthias Kopetzki*

DR. CHRISTOPH SCHMIDT · PROF. DR. SVEND REUSE

# Ansatz zur Prüfung einer adäquaten Risikokultur nach MaRisk 6.0

## Vorstellung eines Quantifizierungsmodells als Basis für eine risikoorientierte Prüfung



**Dr. Christoph Schmidt,** LL.M. (oec.), promovierte am Institut für Corporate Governance der WU Wien und ist Inhaber der auf Interne Revision Outsourcing spezialisierten Unternehmensberatung One More Consulting sowie Lehrbeauftragter für Governance, Risk & Compliance an der Technischen Hochschule Deggendorf.

**Prof. Dr. Svend Reuse,** MBA, ist Bereichsleiter Gesamtbanksteuerung der Stadtparkasse Remscheid, Honorarprofessor an der FOM Hochschule für Ökonomie & Management sowie Fachbeiratsmitglied im isf – Institute for Strategic Finance.

Mit der Veröffentlichung der Mindestanforderungen an das Risikomanagement (MaRisk 6.0) im Oktober 2017 rückt unter anderem das Thema Risikokultur in den aufsichtsrechtlichen Fokus. Eine angemessene Risikokultur ist ab Oktober 2018 als Teil der Ordnungsmäßigkeit der Geschäftsorganisation anzusehen und im Institut zu verankern. Banken- und Finanzdienstleistungsinstitute, insbesondere deren Revisionsabteilungen, stehen vor der Herausforderung, die Angemessenheit der Risikokultur zu bewerten und zu prüfen.

Der vorliegende Artikel beschreibt die aufsichtlichen Anforderungen an eine Risikokultur in Abhängigkeit von Größe und Komplexität der Institute. Hierzu wird ein fragen- oder interviewbasierter Prüfungsansatz vorgestellt, der die Einführung einer adäquaten Risikokultur im Institut überprüft. Auf Basis nationaler und internationaler Indizien wird zudem ein Modell vorgestellt, welches die Umsetzung der Risikokultur im Zeitablauf quantifizieren kann und welches auch für die Revision anwendbar ist.

### 1. Einleitung

Mit der neuen Veröffentlichung der Mindestanforderungen an das Risikomanagement (MaRisk 6.0) durch die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) am 27. Oktober 2017 ergeben sich relevante Veränderungen für Banken- und Finanzdienstleistungsinstitute.<sup>1</sup> Die bis zum 31. Oktober 2018 umzusetzenden Neuregelungen umfassen unter anderem auch die Umsetzung einer angemessenen Risikokultur (AT 3 und AT 5).<sup>2</sup> Nach Auffassung der BaFin ist das Thema nur schwer greifbar.<sup>3</sup> Zudem dürften dem Instrumentarium der Prüfung Grenzen gesetzt sein. Die Aufsicht wird sich jedoch im Zeitverlauf über die Umsetzung der Risikokultur ein Bild machen müssen<sup>4</sup> und betont gleichzeitig den Stellenwert für die Geschäftsleitung.<sup>5</sup> Daher stehen auch Interne Revisionsabteilungen bei Ban-

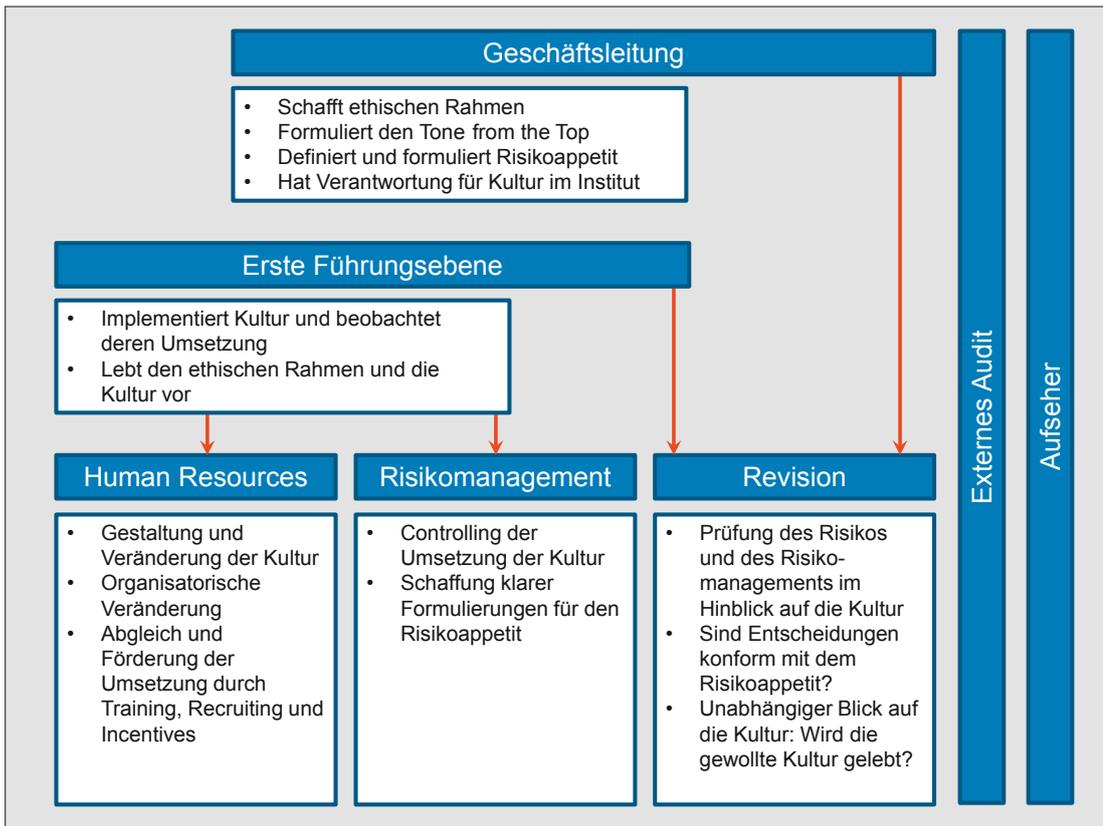
ken und Finanzdienstleistungsinstituten – auch unter Berücksichtigung entsprechender Grenzen – vor der Hausforderung der Prüfung einer angemessenen Risikokultur. Um eine Prüfung zu ermöglichen, sind zunächst die Anforderungen an eine angemessene Ausgestaltung der Risikokultur zu konkretisieren. Ausgehend von der Definition der Risikokultur ist Ziel des Beitrags, Determinanten an eine angemessene Risikokultur nach MaRisk 6.0 darzustellen, einen größen- und komplexitätsinduzierten Umsetzungsplan zu erstellen und einen darauf basierenden Prüfungsansatz abzuleiten.

### 2. Regulatorischer Hintergrund

#### 2.1 Erste Indizien im Prüfungswesen

Ein erstes Indiz für die Definition im Prüfungswesen ist im Prüfungsstandard des Instituts der Wirtschaftsprüfer (IDW) 981 vorzufinden. Demnach wird Risikokultur als Teil der Unter-

1 Vgl. Schmidt, C./Reuse, S. (2018), S. 2.  
2 Vgl. BaFin (2017a), S. 1.  
3 Vgl. BaFin (2017a), S. 4.  
4 Vgl. Hirschmann, S. (2017), S. 42ff.  
5 Vgl. BaFin (2017a), S. 4.



**Abb. 1:**  
Voraussetzungen für eine angemessene Risikokultur<sup>13</sup>

nehmenskultur verstanden.<sup>6</sup> Der Begriff umfasst die grundsätzliche Einstellung und die Verhaltensweise beim Umgang mit Risikosituationen und beeinflusst wesentlich das Risikobewusstsein im Unternehmen. Die Risikokultur in einem Unternehmen stellt die Grundlage eines effektiven Risikomanagementsystems (RMS) dar.<sup>7</sup> Ohne eine angemessene Risikokultur dürfte auch kein wirksames RMS vorhanden sein. Auch aus Sicht des Institute of Internal Auditors (IIA) hat die Aufsicht die Bedeutung einer guten Risikokultur für eine starke Governance erkannt.<sup>8</sup> Nach dem Verständnis des IIA ist die Risikokultur die Gesamtheit von gemeinsamen Werten und Verhaltensweisen von Einzelpersonen in einer Organisation bezüglich des Risikomanagements.<sup>9</sup> Auch das IIA sieht in der Risikokultur ein Kernelement zur Zielerreichung einer Unternehmung.<sup>10</sup> Ethisches und verantwortungsbewusstes Handeln sei aus Sicht des Corporate-Governance-Rates der Australian Securities Exchange (ASX) der Schlüssel zu einer starken Governance. Gleichzeitig bedeutet

die Einhaltung weitaus mehr, als nur die rechtlichen Normen zu berücksichtigen.<sup>11</sup>

## 2.2 Voraussetzung für eine angemessene Unternehmens- und Risikokultur

Die aktuell viel diskutierte Risikokultur ist Teil einer angemessenen Unternehmenskultur. Eine Orientierung für die Voraussetzung einer angemessenen Risikokultur bietet das sogenannte Three-Lines-of-Defense-Modell. Das IIA greift dabei einen klaren ethischen Rahmen auf. Die Einführung und Verankerung dieses Rahmens kann demnach nicht ausschließlich Aufgabe der Geschäftsleitung sein, sondern wird alle Bereiche betreffen. Nach dem britischen Finanzberichterstattungsrat wird die Unternehmenskultur von der Geschäftsleitung festgelegt und unter anderem die Personalabteilung, die Interne Revision und die Risiko- und Compliance-Managementfunktion mit Ressourcen ausgestattet, mit dem Ziel, die Kultur und Werte zu verankern.<sup>12</sup> Aus Abbildung 1 lässt sich unter den Teilbereichen Risikomanagement die Einführung der Risikokultur und die Definition des Risikoappetits ersehen. Die Überprüfung der Einhaltung übernimmt die Interne Revision.

6 Vgl. IDW (2017), S. 10; Berger, T. (2015), S. 645.

7 Vgl. IDW (2017), S. 10, 61.

8 Vgl. Chartered Accountants Australia New Zealand et al. (2017), S. 5.

9 Vgl. Chartered Accountants Australia New Zealand et al. (2017), S. 10.

10 Vgl. Chartered Accountants Australia New Zealand et al. (2017), S. 5.

11 Vgl. Chartered Accountants Australia New Zealand et al. (2017), S. 9.

12 Vgl. Chartered Accountants Australia New Zealand et al. (2017), S. 5

Tz.	MaRisk 6.0	Institute		Klassifizierung		Analyse			
	Wesentlicher Inhalt	syst.rel.	alle	Klarst.	Neu	Aufwand	Rhythmus	Würdigung	Fazit
AT 3 (1)	<b>Risikokultur</b> Die Geschäftsleitung soll die Risikokultur fördern. Analog der Compliance-Kultur ist auch eine Risikokultur einzurichten, die Mitarbeiter sensibilisieren und ein risikoadäquates Verhalten initiieren soll.		X		X	hoch	einmalig	Die Schaffung der Risikokultur ist schlecht messbar und auch nur über einen langwierigen Prozess im Rahmen der Unternehmenskultur machbar. Der Aufwand ist entsprechend nicht zu unterschätzen.	☺
AT 3 (1) Erl.	<b>Kriterien für eine angemessene Risikokultur</b> 1. Tone from the Top: klares Bekenntnis der Geschäftsleitung zu risikogemessenem Verhalten. 2. Die strikte Beachtung des Risikoappetits durch alle Mitarbeiter. 3. Ein transparenter und offener Dialog innerhalb des Instituts zu risikorelevanten Fragestellungen.		X		X	mittel	laufend	Die Konkretisierung ist zu begrüßen, zumal sie erste Anhaltspunkte für die Umsetzung einer Risikokultur geben. Letztlich ist dies ein laufender Prozess, der das Unternehmen aber effizienter machen wird.	☺
AT 5 (3)	<b>Inhalte der Orgarichtlinien</b> Diese müssen nun auch einen Verhaltenskodex für die Mitarbeiter beinhalten – abhängig von der Größe des Instituts sowie der Art, des Umfangs, der Komplexität und des Risikogehalts der Geschäftsaktivitäten.		X		X	mittel	laufend	Die reine Dokumentation des Kodex ist nicht aufwendig – die möglicherweise anstehende Umsetzung von Verhaltensänderungen hingegen sehr wohl. Positiv zu erwähnen ist die eingeführte <b>Öffnungsklausel</b> , welche den Umsetzungsaufwand gerade für kleinere Häuser reduzieren wird.	☺

Abb. 2: Anforderungen an eine angemessene Risikokultur nach MaRisk 6.0<sup>21</sup>

### 2.3 Aufsichtsrechtliche Definition einer Risikokultur

Aufsichtsrechtlich hat das Basel Committee of Banking Supervision (BCBS) eine Definition der Risikokultur gegeben. Das BCBS hat mit der Veröffentlichung der Guidelines – Corporate governance principles for banks im Juli 2015 den Begriff der Risikokultur umfassend definiert.<sup>14</sup> Diese Definition hat die EBA am 15. März 2018 nahezu unverändert übernommen. Demnach umfasst die Risikokultur einer Bank „[d]ie Normen, Einstellung und Verhaltensweisen eines Instituts in Zusammenhang mit Risikobewusstsein, Risi-

kobereitschaft und Risikomanagement sowie die 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.“<sup>15</sup>

Eine weitere Definition zur Risikokultur ist in den MaRisk vorzufinden. Nach AT 3 Tz. 1 wird unter Risikokultur „die Art und Weise [verstanden], wie Mitarbeiter des Instituts im Rahmen ihrer Tätigkeit mit Risiken umgehen (sollen).“<sup>16</sup> In diesem Zusammenhang soll die Identifizierung und das Risikobewusstsein gefördert werden.<sup>17</sup> Es soll sichergestellt werden, dass im Rahmen des

13 In Anlehnung an Chartered Accountants Australia New Zealand et al. (2017), S. 5.

14 Vgl. BCBS (2015), S. 2; diskutiert in Schmidt, C./Reuse, S. (2018), S. 2; ausführlicher dargestellt in Schmidt, C. (2017), Abbildung 1.

15 EBA (2018), Tz. 14, S. 5; Ausführlich dargestellt in Schmidt, C. (2017), Abbildung 2.

16 BaFin (2017b), AT 3, Tz. 1 Erl.

17 Vgl. BaFin (2017b), AT 3, Tz. 1 Erl.

Entscheidungsprozesses Risikogesichtspunkte ausgewogen Berücksichtigung finden.<sup>18</sup>

Werden diese Definitionen der Risikokultur miteinander verglichen, so kann festgehalten werden, dass eine nahezu deckungsgleiche Bedeutung vorliegt, wenngleich die Definition der MaRisk am griffigsten erscheint.<sup>19</sup>

#### 2.4 Anforderungen an eine angemessene Risikokultur nach MaRisk 6.0

Mit der Veröffentlichung der MaRisk 6.0 im Oktober 2017 durch die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) wird eine angemessene Risikokultur als Teil einer ordnungsgemäßen Geschäftsorganisation nach § 25a KWG angesehen. Erste Hinweise hierzu ergeben sich aus AT 3 und AT 5 der MaRisk. Abbildung 2 stellt die Anforderungen der MaRisk 6.0 dar.

Im Sinne einer ordnungsgemäßen Geschäftsorganisation und nach den Vorgaben der BCBS soll die Geschäftsleitung eine angemessene Risikokultur fördern. Als Voraussetzung hierfür sind im Sinne einer risikoorientierten Unternehmensführung die organisatorischen Verantwortlichkeiten zu definieren. Dies kann zu einem Verhaltenskodex führen, der einen wertvollen Beitrag zu einer angemessenen Risikokultur liefern könnte. Die Ausgestaltung ist dabei aus Sicht der Aufsichtsbehörden in Abhängigkeit zur doppelten Proportionalität zu sehen und ist somit bei kleineren Instituten verzichtbar.<sup>20</sup>

Eine Legaldefinition für kleine Institute findet sich in der einschlägigen Fachliteratur nicht. Hierbei sind mehrere Grenzen im Raum. Die FINREP fokussiert drei Milliarden Euro Bilanzsumme.<sup>22</sup> Diese Argumentation wird auch seitens der Bundesbank unterstützt.<sup>23</sup> Entwürfe der CRR aus 2016/2017 bringen Größenordnungen von 1,5 bis 4,6 Milliarden Euro ins Spiel.<sup>24</sup> Der aktuelle Stand per 28. Juni 2018 definiert sogar fünf Milliarden Euro als quantitative Größe.<sup>25</sup> Neben der reinen Größe des Instituts sind aber auch Art, Umfang und Komplexität des Risikogehaltes der Geschäftsaktivitäten maßgeblich.<sup>26</sup> An dieser Stelle

sind die Institute gut beraten, eine für sich passende Analyse durchzuführen und sich nicht nur auf die Bilanzsumme zu fokussieren.

Die Abstufungen können aus Sicht der Autoren unter Berücksichtigung der doppelten Proportionalität zu einer differenzierten Umsetzung führen. Abbildung 3 stellt die Umsetzungsschritte bei der Einführung einer Risikokultur in Abhängigkeit von der obigen Klassifizierung dar.

Ausgehend von der Diskussion um die Größe eines Instituts ist im Rahmen der Erleichterungen für die Risikokultur primär im Bereich der MaRisk für kleinere Institute ein Verhaltenskodex verzichtbar. Aber auch unter Berücksichtigung der Entbehrlichkeit eines Verhaltenskodex ist jedoch eine kontinuierliche interne Kommunikation über Risikoprobleme unter Einbeziehung der Risikostrategie eines Bank- oder Finanzdienstleistungsinstituts erforderlich.<sup>28</sup>

Darüber hinaus greift die Aufsicht weitere Kernelemente auf. Nach BCBS ist die variable Vergütung für die Unterstützung des Risikomanagements und die Unternehmensführung zu nennen. Dabei wird vorausgesetzt, dass die Vergütungsstrukturen sich im Einklang mit der Geschäfts- und Risikostrategie befinden. Ziel dieser vergütungsbezogenen Anreizsysteme ist es, Interessenkonflikte zu minimieren.<sup>29</sup>

### 3. Prüfung der Umsetzung einer adäquaten Risikokultur

#### 3.1 Prüfungsansatz

Internationale Papiere greifen vier Einflussfaktoren auf, die zu einer angemessenen Risikokultur führen können: Leitungskultur, Kommunikation, Verantwortlichkeit und Anreizsysteme. Die MaRisk selbst fokussieren sich nur auf die ersten drei Aspekte, da die Anreizsysteme in der InstitutsVergV geregelt sind. Gleichwohl sind diese Anforderungen eng mit denen der MaRisk verwoben. Es bietet sich folglich auch im Rahmen der Prüfungshandlungen an, MaRisk 6.0 und InstitutsVergV zusammen zu prüfen.

Einen etablierten Prüfungsansatz gibt es, aufgrund der erst jungen Anforderungen, noch nicht. In diesem Zusammenhang besteht die Möglichkeit, sich einerseits Kontrollfragen zu bedienen, die durch zusätzliche Interviews untermauert

18 Vgl. BaFin (2017b), AT 3, Tz. 1; Schmidt, C./Reuse, S. (2018), S. 3.

19 Vgl. Schmidt, C./Reuse, S. (2018), S. 3.

20 Vgl. BaFin (2017a), S. 4.

21 Vgl. Reuse, S. (2016), S. 2; Anlage 1, S. 1 u. 4; Reuse, S. (2017) und Schmidt, C./Reuse, S. (2018), S. 2.

22 Vgl. FINREP (2015), Art.13 (7) a).

23 Vgl. Deutsche Bundesbank (2017), S. 58.

24 Vgl. CRR II-E (2016), Art. 430a (4); CRR II-E (2017), Art. 4 (1) Nr. 144a. Umfassend diskutiert in DSGVO (2018), S. 28.

25 Vgl. CRR II-E (2018), Art. 4 (1) Nr. 144a.

26 Vgl. umfassend CRR II-E (2018), Art. 4 (1) Nr. 144a, d, e, f, g, h.

27 Eigene Darstellung; die Klassifizierungen und Umsetzungs-ideen stellen die persönliche Meinung der Autoren dar.

28 Vgl. BCBS (2015), Tz. 126, S. 30; Schmidt, C./Reuse, S. (2018), S. 9.

29 Vgl. Schmidt, C./Reuse, S. (2018), S. 3.

Umsetzungsschritte	Kleines und wenig komplexes Institut		Mittelgroßes und mittelkomplexes Institut		Systemrelevantes Institut, A-SRI (> 20 Mrd. €)	
Tone from the Top	ja	Das klare Bekenntnis der Geschäftsleitung ist Kern einer jeden Risikokultur und nach Möglichkeit schriftlich zu verankern.	ja	Diese Anforderung ist größenklassenunabhängig umzusetzen.	ja	Auch eine Kommunikation in Richtung Shareholder und Stakeholder ist sinnvoll, da es sich hierbei oft um kapitalmarkt- oder gar börsennotierte Institute handelt.
Tone from the Middle	i. d. R. nein	Je nach Größe des Institutes sind die Wege so kurz oder das Middle Management gar nicht vorhanden, so dass der Tone from the Middle entfallen kann.	ja	Bei komplexeren Hierarchien ist schnell der Punkt erreicht, ab dem die echte Umsetzung der Kultur nicht mehr direkt durch die Geschäftsleitung, sondern durch die zweite Führungsebene erfolgt. Ein Tone from the Middle ist dann erforderlich.	ja	Bei dieser Größe ist die Geschäftsleitung für den einzelnen Mitarbeiter kaum wahrnehmbar. Ein Tone from the Middle auch bis zur dritten oder gar vierten Führungsebene ist kaskadisch erforderlich.
Umsetzung aller Aspekte der InstitutsVergV im Hinblick auf Anreizsysteme	nein	Erst ab 15 Mrd. € gilt ein Institut gem. § 17 InstitutsVergV als bedeutend und muss die Anforderungen der §§ 18 ff. erfüllen.	nein	Erst ab 15 Mrd. € gilt ein Institut gem. § 17 InstitutsVergV als bedeutend und muss die Anforderungen der §§ 18 ff. erfüllen.	i. d. R. ja	A-SRI und bedeutende Institute gem. InstitutsVergV fallen oft zusammen. Die Lücke zwischen 15 und 20 Mrd. € wird an dieser Stelle vernachlässigt.
Sichtung des Risikoappetits und Kopplung mit der Risikokultur	ja	Zumindest Gesamthauslimite und deren Auslastung sowie Größenklassen im Kreditgeschäft sollten verankert werden.	ja	Weitere Risikoappetitdefinitionen sind denkbar, je nachdem, wie komplex die zugrundeliegende Risikostrategie aufgebaut ist.	ja	Ausweitungen in Richtung Reputationsrisiko und strategisches Risiko sind zu empfehlen.
Anpassung Risikostrategie: Ergänzung um Risikokultur	ja	Risikokultur und Risikostrategie sind eng miteinander verwoben. Es bietet sich an, 3–4 Passagen zur Formulierung des Tone from the Top und 1–2 Ziele auf Gesamthausebene in die Risikostrategie aufzunehmen.	ja	Neben den Gesamthauszielen kann die Risikostrategie auch Ziele für die wesentlichen Geschäftsaktivitäten im Hinblick auf die Risikokultur enthalten.	ja	Es bietet sich zusätzlich an, ein für die Mitarbeiter verständliches, separates Dokument zu erstellen. In diesem sind die Essenzen der Risikostrategie für die jeweiligen Bereiche herunterzubrechen.
Verankerung des Verhaltenskodex gemäß AT 5, Tz. 3	nein	Die Öffnungsklausel kann von den Instituten in Anspruch genommen werden. Bei kleinen Instituten ist die persönliche Ansprache der Mitarbeiter durch die Führungskräfte des Instituts das direktere und im Zweifel auch effektivere Mittel (BaFin (2017a), S. 4).	ja	[B]ei größeren Instituten mit weiter verzweigten Geschäftsaktivitäten [ist] ein sinnvolles Instrument (BaFin (2017a), S. 4).  Ein Verhaltenskodex ist schriftlich zu formulieren und auch adäquat zu kommunizieren.	ja	Dies gilt verstärkt für sehr große Institute, die ggf. sogar länderübergreifend in mehreren Sprachen einen solchen Kodex formulieren müssen.
Qualitative Analyse der Risikokultur, erstmalig und laufend	ja	Die Analyse der Risikokultur kann im ersten Schritt über eine qualitative Analyse erfolgen, die auf Negativbeispiele abzielt. Gibt es Gründe/Aspekte, die gegen die adäquate Umsetzung einer Risikokultur sprechen? Ist Fehlverhalten beobachtbar? Halten sich die Mitarbeiter an den definierten Risikoappetit?	ja	Dies kann erweitert werden um eine Art Positivliste: Sind auch Einhaltung der Risikokultur spürbar?	ja	Letztlich kann die qualitative Analyse hier nur der erste Schritt sein – eine quantitative Analyse (s. u.) wird empfohlen.

Fortsetzung nächste Seite

Umsetzungsschritte	Kleines und wenig komplexes Institut		Mittelgroßes und mittelkomplexes Institut		Systemrelevantes Institut, A-SRI (> 20 Mrd. €)	
Sensibilisierung und ggf. Schulung der Mitarbeiter	ja	Durch die kurzen Wege im Haus und die wenig komplexen Ziele in der Risikostrategie sind Schulungen in der Regel nicht notwendig, wenn der Tone from the Top adäquat kommuniziert wird. Allerdings sind Sensibilisierungen trotzdem permanent erforderlich.	ja	Es bietet sich zusätzlich eine einmalige Information der Mitarbeiter zum Schluss des Projektes an, um den Tone from the Top und/oder Middle sowie das gewünschte Verhalten zu formulieren.	ja	Zusätzlich bieten sich regelmäßige Workshops für betroffene Mitarbeiter an.
Initial- und Folgequantifizierung der Risikokultur analog des Modells Schmidt/Reuse	nein	Das in Schmidt/Reuse vorgestellte Quantifizierungsmodell ist für diese Institute nicht zwingend erforderlich – gleichwohl würde es Erkenntnisse bieten, die die Umsetzung einer adäquaten Risikokultur fördern.	ja	Eine Quantifizierung mit dem vorgestellten Modell kann helfen, Schwächen im Haus aufzuzeigen und diese zu beheben. Eine regelmäßige Quantifizierung ist aus Sicht der Autoren empfehlenswert, um die Einhaltung der Risikokultur auch im Zeitablauf sicherzustellen.	ja	Aufgrund der komplexen Aufbau- und Ablauforganisation einer solchen Bank ist das vorgestellte Modell in Schmidt/Reuse nahezu die einzige aktuell vorhandene Methode, eine Risikokultur adäquat zu messen. Eine regelmäßige Quantifizierung bietet sich vor allem aufgrund der sich häufig ändernden Strukturen an.
Definition zusätzlicher Ad-hoc-Mitteilungen bei Verstoß gegen Risikokultur	nein	Ad-hoc-Mitteilungen sind bei kurzen Wegen im Unternehmen nicht zwingend erforderlich. Da oftmals nur Limite oder Abweichungen im Rahmen der Kreditgrößenklassen betroffen sind, werden Ad-hoc-Meldungen bereits über bestehende Regelungen ausgelöst und bedürfen keiner separaten Definition.	nein	Dies wird auch in mittleren Instituten der Fall sein, da auch hier die risikostrategischen Aspekte bereits mit Ad-hoc-Meldepflichten ausgestattet sind.	ja	Verstöße gegen die oben beschriebenen separaten Dokumente für Mitarbeiter sind klar genug definierbar, um neben reinen Limitüberschreitungen auch Ad-hoc-Meldungen zu generieren. Hierzu kann auch eine Art Whistleblowing zählen, die das Fehlverhalten von Mitarbeitern oder Führungskräften Ad-hoc-pflichtig macht.
Aufnahme in das Strategiecontrolling	ja	Eine qualitative Aussage, ob und inwieweit die Risikokultur eingehalten wird, ist ausreichend.	ja	Eine (auch quantitative) Darstellung der Risikotoleranzen, welche verletzt wurden und eine Begründung für die Abweichungen bietet sich hier an.	ja	Aufgrund der Größe des Hauses sollten dezentrale Verstöße gegen die Risikokultur gesammelt und beim Leiter der Risikocontrollingfunktion gebündelt werden, um hier ein umfassendes Strategiecontrolling aufzubauen.

Abb. 3: Umsetzung der Risikokultur im Rahmen der doppelten Proportionalität<sup>27</sup>

ert werden können.<sup>30</sup> Jede Determinante der Umsetzung der Risikokultur ist mit solchen Kontrollfragen versehen, die in Abhängigkeit zu Umfang, Größe und Komplexität des Instituts zu sehen sind.

Darüber hinaus stehen die Prüfungsfelder in Abhängigkeit zur Größenklassifizierung eines Instituts, wie in Abbildung 3 dargestellt. Handelt es sich um ein kleines und wenig komplexes Institut, ist aus Sicht der Aufsicht die Verschriftlichung

des Verhaltenskodex entbehrlich. Anstelle des Verhaltenskodex führt die Aufsicht an, dass der Verhaltenskodex durch „die persönliche Ansprache der Mitarbeiter durch die Führungskräfte des Instituts das direktere und im Zweifel auch effektivere Mittel ist, die Mitarbeiter auf die gemeinsamen Werte und Ziele einzuschwören.“<sup>31</sup> Analog bedeutet dies jedoch, dass bis auf den Verzicht auf einen Verhaltenskodex alle Kontrollfragen der vier Determinanten berücksichtigt werden müssen.

30 Vgl. hierzu umfassend Schmidt, C./Reuse, S. (2018), S. 4 ff. und die dort angegebenen Quellen.

31 BaFin (2017a), S. 4.

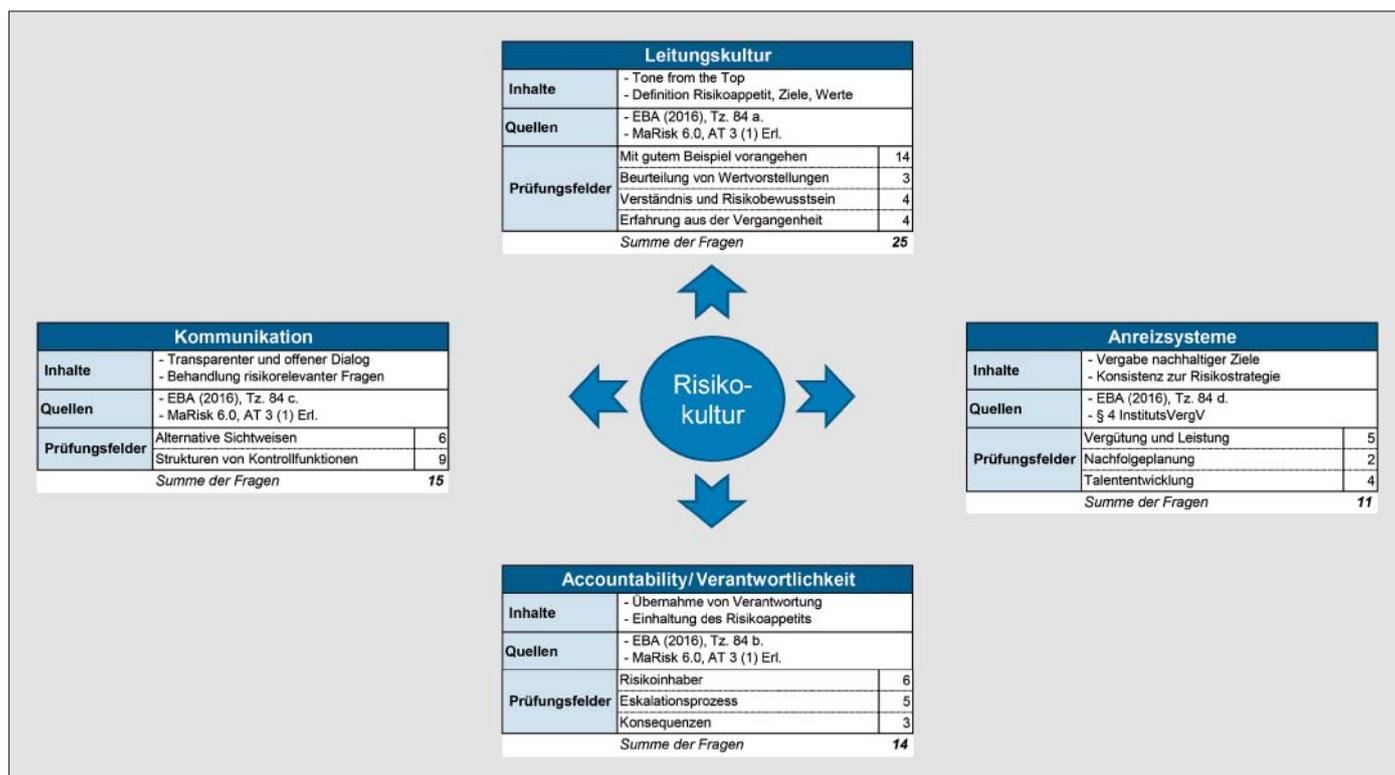


Abb. 4: Prüfungsfelder einer angemessenen Risikokultur<sup>32</sup>

Abbildung 4 visualisiert die vier Prüfbereiche und die Prüffelder, in denen Kontrollfragen gestellt werden können.

In Summe sind es in diesem Beispiel 65 Fragen,<sup>33</sup> die den Internen Revisor in die Lage versetzen können, die Umsetzung und Einhaltung der Risikokultur zu überprüfen. Auf diese Risikokultur sowie deren Anwendung im Prüfprozess wird im Folgenden näher eingegangen.

### 3.2 Prüfungsfelder einer angemessenen Risikokultur

#### Leitungskultur

Grundvoraussetzung für eine angemessene Risikokultur stellt eine Leitungskultur dar. Hierunter sind Risikoappetit, Ziele und Werte zu definieren. Unter der Konkretisierung des Risikoappetits wird nichts anderes als die bewusste Entscheidung verstanden, in welchem Ausmaß die Geschäftsleitung bereit ist, Risiken einzugehen.<sup>34</sup> Diese Festlegung des Risikoappetits mündet in die Risikostrategie, die mit der Geschäftsstrategie im Einklang stehen muss. Bei Banken und Finanzdienstleistungsinstituten dürften dies vor allem

Gesamthauslimite im Rahmen der Risikotragfähigkeit sein. Ein Eckpfeiler der Leitungskultur muss die Vorbildfunktion der Geschäftsleitung sein, die sich auf die Führungskräfte im Institut auswirken soll. Nur wenn die Geschäftsleitung und ihre Führungskräfte mit gutem Beispiel vorangehen, dürfte sich dieses Verhalten auch auf die Mitarbeiter ohne Führungsverantwortung auswirken.<sup>35</sup>

Ausgehend von den Anforderungen an eine Leitungskultur sollen mögliche Prüfungsfragen kurz skizziert werden. Um eine Leitungskultur zu bewerten, sind die Felder Vorbildfunktion, Wertevorstellungen, Risikobewusstsein und Erfahrung aus der Vergangenheit näher zu betrachten. Im Kern geht es darum, klare Regeln für einen integren und wertorientierten Rahmen zu definieren. Darüber hinaus sind die Geschäfts- und Risikostrategie am Risikoappetit auszurichten und somit im Rahmen der Prüfung ebenso zu bewerten. Es ist beispielsweise zu hinterfragen, ob Ziele, Visionen und Werte im gesamten Institut kommuniziert sind, das Management die Risikokultur vorlebt oder der Prozess des offenen Austausches durch ein Whistleblowing-System gefördert wird.<sup>36</sup>

32 Erweiterte Darstellung in Anlehnung an Schmidt, C./Reuse, S. (2018), S. 4 ff. und die dort genannten Quellen.

33 Vgl. umfassend Schmidt, C./Reuse, S. (2018), S. 4 ff.; zur Quantifizierung vgl. Kapitel 3.3.

34 Vgl. BaFin (2017b), AT 3, Tz. 1; Schmidt, C./Reuse, S. (2018), S. 43.

35 Vgl. Schmidt, C./Reuse, S. (2018), S. 40.

36 Vgl. Schmidt, C./Reuse, S. (2018), S. 5.

### Verantwortlichkeit der Mitarbeiter

Darüber hinaus geht die Verantwortlichkeit der Mitarbeiter bereits aus der Definition der Risikokultur hervor. Demnach umfasst die Art und Weise des Umgangs mit Risiken alle Mitarbeiter eines Instituts. Von daher ist jeder Mitarbeiter in seinem Tätigkeitsfeld ein „kleiner Risikomanager“.<sup>37</sup> Die Verantwortung der Mitarbeiter umfasst mehrere Faktoren. Zunächst ist in der Auf- und Ablauforganisation der Risikoinhaber festzulegen. Die Festlegung allein reicht aber bei Weitem nicht aus, sondern bedeutet mehr. Nach Schmidt/Reuse (2018) müssen bei der Implementierung einer neuen Unternehmenskultur und der damit verbundenen Risikokultur auch alle Mitarbeiter sensibilisiert werden.<sup>38</sup> Darüber hinaus sind Eskalationsprozesse und Konsequenzen weitere Faktoren, die im Rahmen der Accountability festzulegen sind.

Die Prüfungsfragen setzen an folgender Stelle an: Die Verantwortlichkeit der Mitarbeiter setzt voraus, dass die Verantwortlichkeit für das Risiko in der Auf- und Ablauforganisation klar definiert ist und dass mögliche Eskalationswege mit Konsequenzen festgelegt sind. Beispielhaft sollte hinterfragt werden, ob alle Mitarbeiter die Konsequenzen ihres Handelns verstehen, wenn sie nicht analog des Risikoappetits handeln. Ferner kann die Frage herangezogen werden, ob bei Non-Compliance ein Eskalationsprozess definiert ist.<sup>39</sup>

### Offene Kommunikation und kritischer Dialog

Die offene Kommunikation und der kritische Dialog werden in AT 3 Tz. 1 der MaRisk aufgegriffen. Dabei geht es nicht nur um einen einseitigen Austausch von der Geschäftsleitung an die Mitarbeiter (Top down),<sup>40</sup> die Kommunikation soll in einem kritischen Dialog in beide Richtungen münden. Als Beispiel können hierzu unterschiedliche Voten im Kreditgeschäft bei Markt und Marktfolge herangezogen werden. Bei einer Abweichung ist eine kritische Beleuchtung unerlässlich und für den Gesamtprozess wertschöpfend. Eine solche Vorgehensweise kann durch die Geschäftsleitung im Rahmen von Workshops gefördert werden. Nur dadurch wird auf allen Ebenen das Ziel erreicht, eine angemessene Risikokultur umzusetzen.<sup>41</sup> Diese Vorgehensweise ist grundsätzlich in der Aufbau- und Ablauforganisation zu implementieren. Der Verzicht auf einen

Verhaltenskodex bei kleineren Instituten und die dann fehlende Definition des Umgangs mit Risiken bedeutet noch lange nicht, eine effektive und offene Kommunikation und einen kritischer Dialog auszublenden.<sup>42</sup> Ein effektives Risikomanagement nach IDW PS 981, Tz. A27 enthält als Grundelement eine sogenannte Risikokommunikation, deren Prozess nachvollziehbar festgelegt und dokumentiert werden muss.<sup>43</sup> Im Rahmen der Prüfungshandlungen des Jahresabschlussprüfers nach IDW PS 981, Tz. A60 erfordert die Prüfung der Risikokommunikation die Beurteilung der aufbau- und ablauforganisatorischen Vorkehrungen im Unternehmen. In diesem Zusammenhang können beispielsweise die Kommunikationswege und -prozesse analysiert werden. Dabei ist von wesentlicher Bedeutung, dass im Rahmen der Prüfung insbesondere die Risikokommunikation nachvollzogen werden kann.<sup>44</sup>

Prüfungsfragen könnten dabei berücksichtigen, ob und inwieweit eine offene Kommunikation und ein kritischer Dialog vorhanden sind und wie diese Themen gelebt werden. Zu Erreichung eines hohen Reifegrades ist es notwendig, entsprechende Kommunikationsprozesse und -wege in der Auf- und Ablauforganisation zu verankern. Beispielhaft sollte deshalb hinterfragt werden, ob die Geschäftsleitung eine offene Kommunikation fördert, ob der Aufsichtsrat die Risikoberichte auch versteht oder die Leitung der Risikocontrollingfunktion nach AT 4.4.1 MaRisk direkt dem zuständigen Vorstand unterstellt ist.<sup>45</sup>

### Anreizstruktur

Anreize sind in der InstitutsVergV ausführlich geregelt. Mit der Veröffentlichung der MaRisk und der Anforderungen an die angemessene Risikokultur rückt auch das Thema Vergütungssystem in den Blickpunkt. Aus der InstitutsVergV ist zu entnehmen, dass ein Vergütungssystem auch eine Vergütungsstrategie enthalten muss. Diese muss auf die Erreichung der Ziele ausgerichtet sein. In diesem Zusammenhang ist zu beachten, dass das Eingehen von überproportional hohen Risiken ausgeschlossen wird und nicht zu einer Zielübererfüllung beitragen soll.<sup>46</sup>

Im Fokus einer Prüfung könnten alle Stell-schrauben von Interesse sein, die den variablen Vergütungsanteil erhöhen. Hier ist insbesondere auf die Anreizkompatibilität der Bemessungs-

37 Vgl. Hirschmann, S. (2017); Schmidt, C./Reuse, S. (2018), S. 41.

38 Vgl. Schmidt, C./Reuse, S. (2018), S. 41.

39 Vgl. Schmidt, C./Reuse, S. (2018), S. 6.

40 Vgl. Wichert, B. (2017), S. 48.

41 Vgl. Schmidt, C./Reuse, S. (2018), S. 7.

42 Vgl. Schmidt, C./Reuse, S. (2018), S. 7.

43 Vgl. IDW (2017), Tz. A27.

44 Vgl. IDW (2017), Tz. A60.

45 Vgl. Schmidt, C./Reuse, S. (2018), S. 6.

46 Vgl. Schmidt, C./Reuse, S. (2018), S. 7.

**REGELN** Prüfung der Risikokultur in Banken

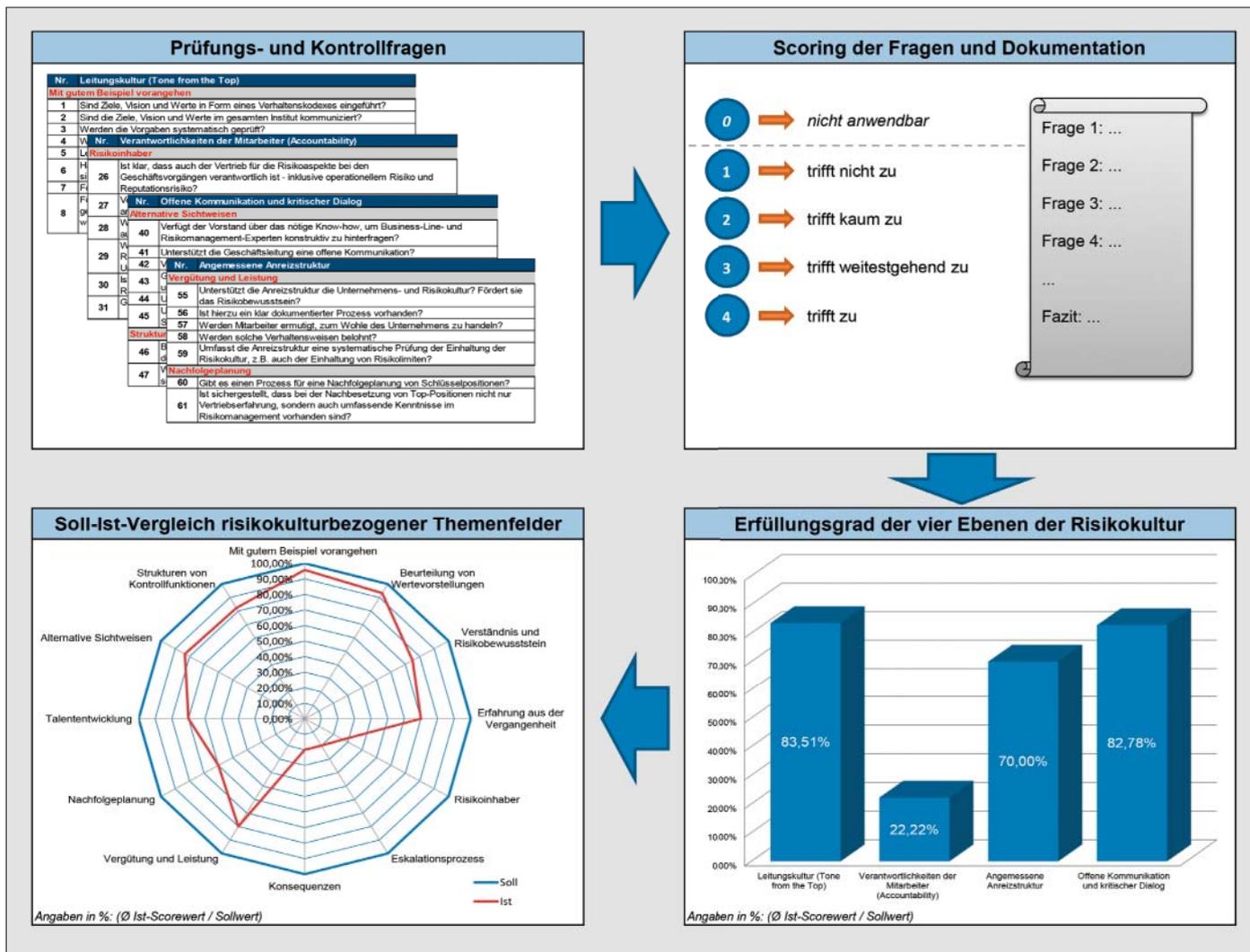


Abb. 5: Quantifizierte Ergebnisse der Prüfungshandlungen<sup>49</sup>

grundlage abzustellen. In der Regel werden variable Vergütungsbestandteile als Leistungsgrößen entlohnt. Im Rahmen einer Prüfung wäre zu hinterfragen, ob Geschäfts- und Risikostrategie mit der Bemessungsgrundlage der Leistungsgrößen kompatibel sind. Exemplarisch könnten wertorientierte Kennzahlen wie EVA (Economic Value Added), RORAC (Return on Risk Adjusted Capital) oder RAROC (Risk Adjusted Return on Capital) herangezogen werden. Wäre eine der ausgewählten Kennzahlen über dem Ziel, käme es zu einer Ausschüttung des variablen Entgeltbestandteils. Als Negativbeispiel ist das Eingehen von hohen Risiken mit der gleichzeitigen Ausschüttung von hohen Vorstandsboni zu nennen. Ziel ist es, mittels der Prüfungsfragen die Nachhaltigkeit des Geschäftsmodells zu beurteilen.

**3.3 Ergebnis der Prüfung für eine angemessene Risikokultur nach MaRisk 6.0**

Der Grundgedanke der doppelten Proportionalität muss auch bei den Prüfungshandlungen im Kontext der Risikokultur wiederzufinden sein. Für kleine und wenig komplexe Banken ist es ausreichend, die Aspekte des Kapitels 3.2 qualitativ zu würdigen und – analog zu Abbildung 3 – mit einem Negativansatz beziehungsweise Ausschlussverfahren vorzugehen. Wenn es Aspekte gibt, die gegen die adäquate Umsetzung einer Risikokultur sprechen, muss tiefergehend geprüft werden. Wird dies verneint, so kann auch in der Prüfung von einer adäquaten Risikokultur ausgegangen werden.<sup>47</sup>

Für die Beurteilung der Angemessenheit der Risikokultur bei einem großen und komplexen In-

<sup>47</sup> Vgl. Schmidt, C./Reuse, S. (2018), S. 7–8.

stitut kann ein sogenanntes Quantifizierungsmodell auf Basis der erwähnten Kontrollfragen eingesetzt werden. Auf Grundlage der FSB Guidelines of Supervision Interaction with Financial Institutions on Risk Culture wurde ein Prototyp entwickelt, um eine Bewertung vornehmen zu können.<sup>48</sup> Ursprünglich für die Messung der Umsetzung der Risikokultur entwickelt, kann er aber auch revisionsseitig Anwendung finden. Der Prototyp enthält dabei die Kontrollfragen aller vorgestellten Determinanten. Mittels der Bewertung auf Basis eines Scoring-Modells (0–4) werden dann die Stärken und Schwächen der derzeitigen Risikokultur aufgezeigt. Das Ergebnis auf Basis fiktiver Daten zeigt Abbildung 5.

Zu erkennen ist, dass in diesem fiktiven Beispiel beim Eskalationsprozess und dem Konsequenzenmanagement erheblicher Nachholbedarf besteht. Dieser Steuerungsimpuls kann Schluss-

folgerung und auch Maßnahmenkatalog im Revisionsbericht sein, um der Geschäftsleitung den nötigen Mehrwert der internen Prüfung zu offerieren. Ein entsprechendes Nachverfolgungsmanagement der Umsetzung dieser Maßnahmen ist dann der nächste Schritt.

Anzumerken ist jedoch, dass eine solche Quantifizierung nur bei mittelgroßen oder größeren Instituten sinnvoll ist. Bei kleinen und wenig komplexen Instituten reichen die Beantwortung einer Auswahl der oben genannten Fragen und ein qualitatives Fazit im Revisionsbericht aus Sicht der Autoren völlig aus. Die doppelte Proportionalität sollte somit nicht nur in der Umsetzung der Risikokultur, sondern gerade auch in der Prüfung Anwendung finden.

#### 4. Fazit

Eine angemessene Risikokultur als Teil der Unternehmenskultur ist Bestandteil eines effektiven Risikomanagementsystems. Vor dem Hintergrund der bekannten Banken Krisen erscheint das Thema wichtiger denn je. Die Verfehlungen in den ver-

48 Umfassend beschrieben in Schmidt, C./Reuse, S. (2018), S. 8–9.

49 Eigene Darstellung in Anlehnung an Schmidt, C./Reuse, S. (2018), S. 8.

gangenen Jahren sind ein Indiz unter anderem für fehlgeleitete Anreizsysteme und die damit eingehenden institutsspezifischen Kultur Aspekte. Die BaFin hat darauf reagiert und mit der Veröffentlichungen der MaRisk im Oktober 2017 die Notwendigkeit einer angemessenen Risikokultur erkannt. Ziel ist es, eine gelebte Risikokultur zu erreichen, deren zeitliche Dimension und Wirkung nicht unterschätzt werden dürfen.

Dieser Artikel hat einen einfachen und doch transparenten Ansatz aufgezeigt, mit dem die Risikokultur seitens der Internen Revision geprüft werden kann. Durch den Prüfungsansatz, basierend auf Kontrollfragen, kann auf qualitative oder auch quantitative Art und Weise die Adäquanz der Risikokultur revisionsseitig bestätigt werden. In Kombination mit den dargestellten Umsetzungserfordernissen im Rahmen der doppelten Proportionalität sind folglich alle Instrumente zur Umsetzung und Prüfung einer Risikokultur vorhanden.

### Literaturhinweise

- BaFin (2017a): Anschreiben zur Veröffentlichung der MaRisk 6.0, GZ: BA 54-FR 2210-2017/0002, 27.10.2017, [https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl\\_rs0917\\_marisk\\_an\\_schreiben\\_pdf\\_ba.pdf?\\_\\_blob=publicationFile&t=3](https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs0917_marisk_an_schreiben_pdf_ba.pdf?__blob=publicationFile&t=3) (Stand: 15.04.2018).
- BaFin (2017b): Rundschreiben 09/2017 (BA) vom 27.10.2017, Anlage 1: Erläuterungen zu den MaRisk in der Fassung vom 27.10.2017, AT 3, Tz. 1 und AT 5, Tz. 2, [https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl\\_rs0917\\_marisk\\_Endfassung\\_2017\\_pdf\\_ba.pdf?\\_\\_blob=publicationFile&t=5](https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs0917_marisk_Endfassung_2017_pdf_ba.pdf?__blob=publicationFile&t=5) (Stand: 15.04.2018).
- BCBS (2015): Guidelines – Corporate governance principles for banks, <http://www.bis.org/bcbs/publ/d328.pdf> (Stand: 15.04.2018).
- Berger, T. (2015): Risikokultur. Das informelle Fundament des Risikomanagements, in: Gleichner, W./Romeike, F. (Hrsg.): Praxishandbuch – Konzepte – Methoden – Umsetzung, Berlin 2015, S. 643–654.
- Chartered Accountants Australia New Zealand, The Ethics Centre, Governance Institute of Australia and Institute of Internal Auditors – Australia (2017): Managing Culture. A good practice guide, Dezember 2017, [http://iia.org.au/sf\\_docs/default-source/default-document-library/424\\_managing-culture-a-good-practice-guide\\_v8.pdf?sfvrsn=2](http://iia.org.au/sf_docs/default-source/default-document-library/424_managing-culture-a-good-practice-guide_v8.pdf?sfvrsn=2) (Stand: 15.04.2018).
- CRR II-E (2016): Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EU) Nr. 575/2013 in Bezug auf die Verschuldungsquote, die strukturelle Liquiditätsquote, Anforderungen an Eigenmittel und berücksich-

tigungsfähige Verbindlichkeiten, das Gegenparteiausfallrisiko, das Marktrisiko, Risikopositionen gegenüber zentralen Gegenparteien, Risikopositionen gegenüber Organismen für gemeinsame Anlagen, Großkredite, Melde- und Offenlegungspflichten und zur Änderung der Verordnung (EU) Nr. 648/2012. CRR II-E (2017): Entwurf eines Berichtes über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EU) Nr. 575/2013 in Bezug auf die Verschuldungsquote, die strukturelle Liquiditätsquote, Anforderungen an Eigenmittel und berücksichtigungsfähige Verbindlichkeiten, das Gegenparteiausfallrisiko, das Marktrisiko, Risikopositionen gegenüber zentralen Gegenparteien, Risikopositionen gegenüber Organismen für gemeinsame Anlagen, Großkredite, Melde- und Offenlegungspflichten und zur Änderung der Verordnung (EU) Nr. 648/2012 (COM(2016)0850 – C8-0480/2016 – 2016/0360A(COD)), <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2F%2FNONGML%2B%2BCOMPARL%2BPE-613.409%2B03%2BDOC%2BPDF%2BV0%2F%2FDE> (Stand: 01.04.2018).

CRR II-E (2018): über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EU) Nr. 575/2013 in Bezug auf die Verschuldungsquote, die strukturelle Liquiditätsquote, Anforderungen an Eigenmittel und berücksichtigungsfähige Verbindlichkeiten, das Gegenparteiausfallrisiko, das Marktrisiko, Risikopositionen gegenüber zentralen Gegenparteien, Risikopositionen gegenüber Organismen für gemeinsame Anlagen, Großkredite, Melde- und Offenlegungspflichten und zur Änderung der Verordnung (EU) Nr. 648/2012 (COM(2016)0850 – C8-0480/2016 – 2016/0360A(COD)), <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONGML+REPORT+A8-2018-0242+0+DOC+PDF+V0//DE> (Stand: 28.07.2018).

Deutsche Bundesbank (2017): Der aufsichtliche Überprüfungs- und Bewertungsprozess für kleinere Institute und Überlegungen zur Proportionalität, in: Monatsbericht, Oktober 2017, S. 45–58, [https://www.bundesbank.de/Redaktion/DE/Downloads/Veroeffentlichungen/Monatsberichtsauftsaetze/2017/2017\\_10\\_aufsichtliche\\_ueberpruefung.pdf?\\_\\_blob=publicationFile](https://www.bundesbank.de/Redaktion/DE/Downloads/Veroeffentlichungen/Monatsberichtsauftsaetze/2017/2017_10_aufsichtliche_ueberpruefung.pdf?__blob=publicationFile) (Stand: 02.04.2018).

DSGV (2018): Mindestanforderungen an das Risikomanagement – Interpretationsleitfaden – Version 6 – April 2018, [http://www.s-wissenschaft.de/kunden/ebusti/xpage/s-wissenschaft.nsf/0/2D49B25D9D45CDBCC12581F0004AC370/\\$FILE/DSGV\\_MaRisk-ILF\\_Version\\_6\\_Internet.pdf](http://www.s-wissenschaft.de/kunden/ebusti/xpage/s-wissenschaft.nsf/0/2D49B25D9D45CDBCC12581F0004AC370/$FILE/DSGV_MaRisk-ILF_Version_6_Internet.pdf) (Stand: 01.05.2018).

EBA (2018): Leitlinien zur internen Governance, EBA/GL/2017/11, 15.03.2018, [https://www.eba.europa.eu/documents/10180/2164689/Guidelines+on+Internal+Governance+%28EBA+GL+2017-11%29\\_DE.pdf/411fdd9d-8174-4366-ab36-3aa9b0a1d716](https://www.eba.europa.eu/documents/10180/2164689/Guidelines+on+Internal+Governance+%28EBA+GL+2017-11%29_DE.pdf/411fdd9d-8174-4366-ab36-3aa9b0a1d716) (Stand: 01.05.2018).

- FINREP (2015): Verordnung (EU) 2015/534 der europäischen Zentralbank vom 17.03.2015 über die Meldung aufsichtlicher Finanzinformationen (EZB/2015/13), <http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32015R0534&from=DE> (Stand: 01.04.2018).
- Hirschmann, S. (2017): Kultur muss ein Thema der Aufsicht sein – Interview mit Ira Steinbrecher und Moritz Römer, in: Die Bank, Heft 03/2017, S. 42–44.
- IDW (2017): IDW Prüfungsstandard: Grundsätze ordnungsmäßiger Prüfung von Risikomanagementsystemen (IDW PS 981), Stand: 03.03.2017, 61. Erg.-Lfg., Juni 2017.
- Reuse, S. (2016): MaRisk 6.0-E – Kritische Analyse des Konsultationsentwurfes vom 18.02.2016 und Anlage: MaRisk 6.0-E – Detailanalyse aller Änderungen, in: Banken-Times Spezial Sonderausgabe MaRisk NEU, Februar 2016, S. 2, Anlage S. 1 u. 4.
- Reuse, S. (2017): MaRisk 6.0 – Würdigung der finalen Version vom 27.10.2017, Darstellung von Umsetzungsempfehlungen und Aufbau eines Projektplans, in: Banken-Times Spezial Sonderausgabe MaRisk – November, <https://www.fc-heidelberg.de/banken-times-spezial-sonderausgabe-marisk-2/?print=print> (Stand: 07.11.2017).
- Steinbrecher, I. (2015): Risikokultur: Anforderungen an eine verantwortungsvolle Unternehmensführung, in: BaFin Journal, August 2015, S. 20–23, [https://www.bafin.de/SharedDocs/Downloads/DE/BaFinJournal/2015/bj\\_1508.pdf?\\_\\_blob=publicationFile&t=2](https://www.bafin.de/SharedDocs/Downloads/DE/BaFinJournal/2015/bj_1508.pdf?__blob=publicationFile&t=2) (Stand: 01.05.2018).
- Schmidt, C. (2017): Anforderungen an eine angemessene Risikokultur, in: Betriebswirtschaftliche Blätter, 23.08.2017.
- Schmidt, C./Reuse, S. (2018): MaRisk 6.0: Ausgestaltung und Quantifizierung einer adäquaten Risikokultur, in: Zeitschrift für das gesamte Kreditwesen, Fritz Knapp Verlag, 71, 05/2018, S. 38–43.
- Wichert, B. (2017): Nachweisspur einer angemessenen Risikokultur, in: Die Bank, Heft 03/2017, S. 46–49.