Beauftragtenwesen

Compliance-Kultur

Die Corporate Governance gerät immer stärker in ein Spannungsfeld zwischen Legalität und Legitimität. Einerseits fordern aufsichtsrechtliche Vorgaben und Novellen eine stärkere Fokussierung auf die Ziele einer robusten Risikokultur, andererseits lassen die hierzu definierten Forderungen eine Reihe von Spielräumen für unternehmerische Entscheidungen zu.

Wo liegt die richtige Balance in der operativen Umsetzung? Nach welchen Maßstäben wird der Regulator künftig urteilen? Und vor allen Dingen: Zahlen sich die Anstrengungen für die Implementierung einer Risikokultur auch monetär aus?

Die Herausforderungen für die Geschäftsleitung eines Kreditinstituts werden immer komplexer. Das betriebswirtschaftliche Umfeld in den aktuellen Zeiten der Niedrigzinsphase, der Wettbewerb durch innovative FinTechs und ein sich kontinuierlich veränderndes Kundenverhalten beschäftigen Vorstände und Geschäftsführer schon seit Jahren. Auch die Flut regulatorischer Initiativen ist längst kein neues Phänomen. Dabei fällt ein neuer Schwerpunkt der (europäischen) Aufsichtsbehörden auf.

Next Best Thing: Corporate Governance

In der Finanzdienstleistungsbranche wurden erste Tendenzen in Richtung „Corporate-Governance-Systeme“ mit der Veröffentlichung des SREP-Prozesses sichtbar. Zwar betrifft der SREP vordergründig nur alle unmittelbar von der EZB beaufsichtigten Institute. Mittelbar ist er jedoch als Grundlage für das deutsche Aufsichtsrecht und die nationale Prüfungspraxis insgesamt von erheblicher Bedeutung. Die EZB hat hierzu bereits – auch für Volksbanken, Raiffeisenbanken und Sparkassen – Anweisungen und Leitlinien aufgestellt. Und tatsächlich haben eine Reihe von Instituten aus unserer Gruppe zwischenzeitlich auch eine Information über einen für sie geltenden SREP-Kapitalzuschlag erhalten.

Aktuell entwickelt die EZB in Zusammenarbeit mit den nationalen Aufsichtsbehörden eine EU-weit geltende SREP-Methodik für die LSIs, die „lokal bedeutenden Institute“. Die entsprechende Konsultation ist für 2018 vorgesehen. Neben den quantitativen Kapital- und Liquiditätsthemen sind dabei auch die Analyse des Geschäftsmodells und die Governance-Regelungen von Bedeutung. Der Umgang mit Kredit-, Liquiditäts- und Marktrisiken – gemeinhin unter dem Begriff des „Financial Risk“ summiert – ist aufgrund seiner weitestgehend mathematischen Natur im Rahmen operativer Umsetzungen praxisnah modellierbar. Das Gegenstück hierzu bilden die sogenannten „Non Financial Risks“, zu denen u. a. die interne Governance, das Reputations- und Compliance-Risiko zählen. Darauf zahlt auch die fast schon nicht mehr erwartete MaRisk-Novelle ein, die seit wenigen Wochen ihre Wirkung entfalten darf.

Tatsächlich finden sich in den MaRisk neben den quantitativen und liquiditätsrelevanten Inhalten auch die Themen Risikokultur und Governance sowie die Auslagerungssteuerung wieder. Sie unterstreichen damit ihrerseits die Bedeutung der unternehmerischen Governance.

Die Wurzeln

Das ist im Kern nicht neu. Spätestens seit Inkrafttreten des Bilanzmodernisierungsgesetzes in 2009 haben kapitalmarktorientierte Kapitalgesellschaften sowie ihnen gleichgestellte Personengesellschaften die wesentlichen Merkmale des internen Kontroll- und Risikomanagementsystems im Hinblick auf den (Konzern-) Rechnungslegungsprozess im (Konzern-)Lagebericht zu beschreiben. Dadurch haben sich auch die Überwachungspflichten des Aufsichtsorganes auf die Wirksamkeit des Internen Kontrollsystems (IKS), des Risikomanagementsystems (RMS) und des Internen Revisionssystems (IRS) verstärkt. Durch die Einführung eines wirksamen Compliance-Management-Systems (CMS) soll eine Art „Klammerfunktion“ geschaffen werden, die sich durch eine effektive Zusammenführung relevanter Kontrollerkenntnisse aller Beauftragtenfunktionen in eine ope- >

rativ wirksame Kontroll- und Steuerungsfunktionalität auszeichnen soll. Das Erkennen, Managen und Berichten identifizierter Risiken und Schwachstellen stellt den Kern dieser Systematik dar.

Somit verwundert es nicht, dass die „European Banking Authority" (EBA) im Rahmen des 2014 veröffentlichten SREP-Prozesses vorgegeben hat, auch die Bewertung der Regelungen zur internen Governance und der institutsweiten Kontrollen der Unternehmen zu prüfen:

- Sind diese Regelungen und Kontrollen angesichts des Risikoprofils, des Geschäftsmodells, der Größe und der Komplexität des Instituts angemessen?
- In welchem Maß hält das Institut die Anforderungen und Standards einer guten Unternehmensführung und einer ordnungsgemäßen Risikokontrolle ein?

Diese Ziele werden unter den Überschriften „Gesamtrahmen für die interne Governance", „Unternehmens- und Risikokultur", „Zusammensetzung und Arbeitsweise des Leitungsorganes", „Vergütungspolitik und -praxis", „Rahmenwerk für das Risikomanagement" und „Interner Kontrollrahmen" in Kapitel 5.1 ff. weiter ausgeführt. Hinsichtlich der jeweiligen Ausgestaltung und des Einsatzes konkreter Hilfsmittel und Techniken werden zwar keine Vorgaben gemacht. Sollten jedoch – nach Ermessen der zuständigen Behörden – die implementierten Strukturen Schwächen aufweisen, kann sich dies sogar in möglichen Kapitalzuschlägen niederschlagen.

Diese Vorgaben hat das Institut der Wirtschaftsprüfer aufgegriffen und im März dieses Jahres u. a. die IDW-Prüfungsstandards IDW EPS 981 und 982 – zusätzlich zu dem IDW 980 und dem IDW 983 – formuliert. Unter der zusammenfassenden Überschrift „Prüfung von Corporate-Governance-Systemen" werden die Grundsätze einer ordnungsgemäßen Prüfung von Risikomanagementsystemen (EPS 981) und des Internen Kontrollsystems der Unternehmensberichterstattung (EPS 982) definiert. Durch die Veröffentlichung der MaRisk-Novelle wird nunmehr noch einmal sehr prominent artikuliert, dass die Umsetzung dieses Themas künftig verstärkt in den Fokus der Behörden rücken wird.

MaRisk unterstreichen die Bedeutung einer Risikokultur

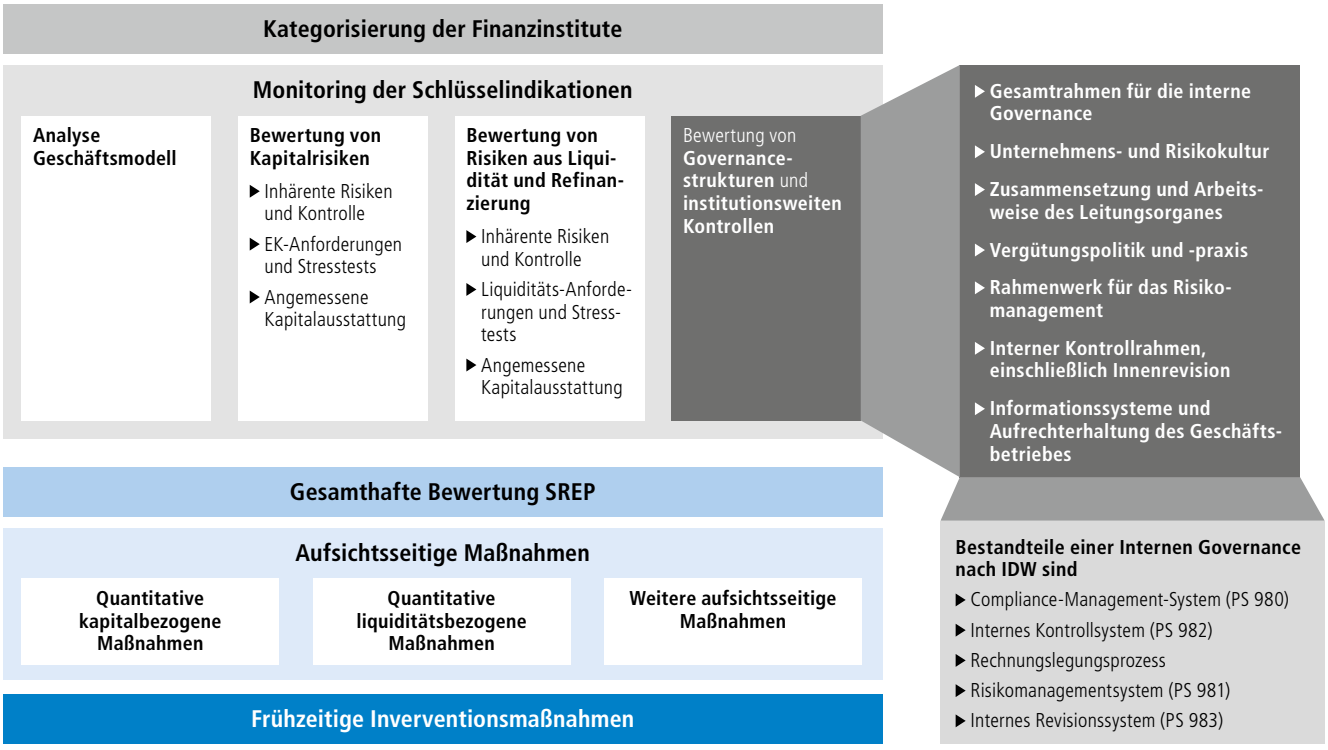
So macht die BaFin im Anschreiben zur Veröffentlichung der MaRisk unmissverständlich deutlich, dass sich die Institute künftig mit der Implementierung einer angemessenen Risikokultur stärker auseinandersetzen müssen.

Schwierig dürfte es jedoch mit der Messbarkeit einer erfolgreichen Risikokultur werden. Die BaFin verweist z. B. auf wünschenswerte sowie angemessene Verhaltensweisen bzw. Praktiken und postuliert dabei auch den möglichen Einsatz eines Verhaltenskodexes. Gleichzeitig jedoch weist sie auf die mögliche Verzichtbarkeit eines solchen Kodexes speziell bei kleineren Instituten und solchen mit weniger komplexen Aktivitäten hin.

Was bedeutet dies nun für die Vorstände eines Unternehmens, wenn sie künftig die Vorgaben der BaFin in einem angemessenen und wirksamen Rahmen etablieren wollen? Worauf konkret werden sie achten müssen und welche Erwartungshaltungen z. B. ihrer Prüfer werden sie erfüllen müssen? Ein Blick in die aufsichtsrechtlichen Veröffentlichungen zu den Themen Risikokultur und Corporate Governance verdeutlicht recht einprägsam, welche Kausalketten und Bedeutungen sich hinter dem Begriff der Risikokultur verbergen. Die Risikokultur und vor allen Dingen die Art und Weise, wie sie etabliert, kontrolliert und gelebt wird, ist essenzieller Bestandteil des Risikomanagements und der institutsspezifischen Corporate Governance. Worum kann es künftig konkret gehen, wenn die Behörden im Rahmen des SREP-Prozesses bewerten, wie „ernst" es einer Unternehmensführung mit der internen Governance und den institutsweiten Kontrollen ist, und wie wird die Aufsicht sich ein Bild über die gelebte Risikokultur in einer Bank verschaffen?

Insoweit ist der Erkenntnisgewinn mit den nun veröffentlichten MaRisk hinsichtlich neuer aufsichtlicher Vorgaben und Kontrollüberlegungen eher gering. Die MaRisk geben (aber) einen Fingerzeig darauf, mit welchen inhaltlichen Schwerpunkten sich die Behörden im Rahmen bereits beste-

Abb. 1 INTEGRIERTE RISIKOKULTUR



hender Vorgaben in der Zukunft (verstärkt) auseinandersetzen werden. Die Unternehmen tun gut daran, die MaRisk nicht als isolierten „Umsetzungsauftrag" zu betrachten. Es empfiehlt sich auch nicht, die sogenannten „weichen", weil überwiegend qualitativen Elemente zur Einführung einer Risikokultur als „theoretischen bzw. philosophischen" Auftrag zu betrachten. Vielmehr erscheint es ratsam, den Umgang über die bislang etablierten Elemente des Risikomanagements, der Governance und deren Operationalisierung hinaus gesamthaft zu betrachten. AT 3 der MaRisk fordert, in Stichpunkten zusammengefasst:

- Alle Geschäftsleiter sind für eine ordnungsgemäße Geschäftsorganisation und deren Weiterentwicklung verantwortlich.
- Alle Risiken müssen beurteilt und durch Sicherungsmaßnahmen begrenzt werden.
- Maßnahmen dazu sind auch die Entwicklung, Förderung und Integration einer angemessenen Risikokultur.
- Jeder Geschäftsleiter ist für die Einrichtung angemessener Kontroll- und Überwachungsprozesse in seinem jeweiligen Zuständigkeitsbereich verantwortlich.
- Die Risikokultur beschreibt
  - wie Mitarbeiter des Instituts im Rahmen ihrer Tätigkeit mit Risiken umgehen,
  - ein klares Bekenntnis der Geschäftsleitung zu risikoangemessenem Verhalten,
  - die Wichtigkeit Entscheidungsprozesse unter Risikogesichtspunkten ausgewogen durchzuführen,
  - die strikte Einhaltung eines einmal kommunizierten Risikoappetits,
  - die Ermöglichung und Förderung eines transparenten Dialogs.

Abbildung 1 verdeutlicht die Zusammenhänge. >

Compliance-Management-System: Zahlt es sich aus?

Ein detailliertes Studium der zuvor erwähnten Standards und Rahmenbedingungen fördert eine ganze Reihe identischer Begriffspaare und Vorgaben zutage. Dies verdeutlicht, dass mit einer intelligenten Umsetzung der MaRisk viele Aufgaben gleichzeitig und mit einem größeren Nutzen als bislang möglich umgesetzt werden können. Damit aber nicht genug.

Tatsächlich lohnen sich Investitionen aus Sicht der Corporate Governance in ein Compliance-Management-System auch finanziell. Der Einfluss auf mögliche Kapitalzuschläge im Rahmen des SREP-Prozesses wurde bereits herausgearbeitet. Dieser ist zweifellos aufgrund seiner kontinuierlichen Wirkungsweise – basierend auf einer jährlich wiederkehrenden Bewertung – künftig auch für LSIs von nicht unerheblicher Bedeutung.

Seit wenigen Monaten gibt es aber eine finanziell zusätzlich relevante Herausforderung, die mit einem funktionierenden Compliance-Management-System in direkter Verbindung steht. Unter dem Aktenzeichen 1 StR 265/16 vom 9. Mai 2017 hat der BGH mit seinem Urteil einen Meilenstein in Bezug auf die bußgeldmindernde Wirkung eines Compliance-Management-Systems begründet. Hintergrund des Urteils ist, dass ein deutsches Unternehmen ein Geschäft getätigt hat, das auf unzulässigen Absprachen beruhte und in dessen Zusammenhang Provisionen gezahlt wurden. Diese wurden fälschlicherweise als Betriebsausgaben deklariert. Dabei wies der BGH als Revisionsinstanz wie folgt auf die bußgeldmindernde Wirkung eines Compliance-Management-Systems hin:

- Für die Bemessung einer Geldbuße ist es u. a. bedeutend, inwieweit ein Unternehmen seiner Pflicht, Rechtsverletzungen aus der Sphäre des Unternehmens zu unterbinden, genügt und ein effizientes Compliance-Management-System installiert hat.
- Das Compliance-Management-System muss auf die Vermeidung von Rechtsverstößen ausgelegt sein (also präventiv wirken).
- Selbst die Bemühungen um eine Optimierung von Regelungen und betriebsinternen Abläufen, die nach einer Normverletzung vorgenommen werden, können sich strafmindernd auswirken, wenn sie darauf ausgelegt werden, zukünftige vergleichbare Normverletzungen deutlich zu erschweren.

Dieses Urteil ist Balsam auf die aufwandsgeschundene Seele der durch überbordende Regulierung geplagten Unternehmenslenker. Die enormen Anstrengungen, ein Compliance-

AUTOR UND ANSPRECHPARTNER

Andreas Marbeiter
Geschäftsführung,
E-Mail: andreas.marbeiter@geno-tec.de

Management-System zu implementieren und zu optimieren, werden nunmehr im Falle eines Falles honoriert. Im Zeitalter sich ständig verschärfender Strafzahlungen ist dies hochwillkommen. Allerdings: Das Compliance-Management-System darf nicht nur auf dem Papier die rechtlichen Anforderungen an das Compliance-Management-System erfüllen. Es müssen auch die damit verbundenen Prozesse identifiziert und laufend optimiert werden.

Am Ende geprüft

Wie bereits eingangs erwähnt, unterstreicht das IDW die Bedeutung eines effizienten Compliance-Management-Systems und der damit verbundenen Einführung einer robusten Risikokultur. Es hat die bereits erwähnten Standards für freiwillige Prüfungen der Governance-Elemente (EPS 981 und EPS 982) definiert, welche die Jahresabschlussprüfung ergänzen, die nur bedingt Fragen zur Angemessenheit der Governance-Struktur beantwortet.

Die neuen Standards dienen gleichzeitig und insbesondere als Orientierungshilfe für Vorstände und Aufsichtsräte für Governance-Strukturen. Die Ergebnisse dieser freiwilligen Prüfungsberichte werden auch den Aufsichtsgremien wesentliche Hinweise zur Governance liefern können. Schließlich sind sie das Fundament einer Governance-Bewertung in den überwachten Unternehmen. Die Berichte können somit wichtige Impulse bei der Bewertung der Governance in den durch die Aufsichtsräte überwachten Unternehmen geben.

Es liegt an den Vorständen selbst, in welcher Form sie sich mit den etablierten Abläufen beschäftigen und wie sie darauf achten, dass die Compliance-Kultur im Unternehmen tatsächlich gelebt und beurteilt wird. Um jedoch im Rahmen des (künftigen) SREP-Prozesses und auch (für den Fall der Fälle) im Rahmen eines OWiG-Verfahrens bestehen zu können, bedarf es einer nachhaltig dokumentierten Herangehensweise. Deren Umfang und Intensität ist abhängig von Art, Umfang, Komplexität und Risikogehalt der Geschäftsaktivitäten.

Zentrale Umsetzungsunterstützung

Das abgestufte Vorgehensmodell trägt der genossenschaftlichen Werteleitlinie und damit den Governance-Strukturen der genossenschaftlichen Kreditinstitute mit ihren unterschiedlichen Größenordnungen und Geschäftsstrukturen Rechnung. Es muss also nur noch „irgendwie“ gelingen, das „Leben“ der Risikokultur messbar zu machen und es zu dokumentieren.

Unsere Ad-hoc-Lösung ist, dass wir unsere Vor-Ort-Besuche im Rahmen der einzelnen Beauftragtenfunktionen bereits heute auf diesen speziellen Blickwinkel ausgerichtet haben.

Gleichzeitig investieren wir in die Entwicklung entsprechender Vorgehensmodelle und intensivieren in Bezug auf eine Governance insgesamt unsere Überlegungen, wie wir – als Mehrmandantenanbieter – Sie unterstützen können. Dabei verfolgen wir das Ziel, dass die GenoTec-Dienstleistungen Ihnen als Bank helfen, prüferisch verwertbare Dokumentationen zu generieren, aufgrund derer ein effizientes Compliance-Management-System auch einen dokumentierten Faktor für eine robuste, gelebte Risikokultur darstellt. ▬