Harald Lob

Erste, zweite und dritte Verteidigungslinie als Kernstück der **Regulierung** – wer verteidigt was?

Aus den Erfahrungen der Finanz- und Wirtschaftskrise seit 2008 sind zahlreiche regulatorische Maßnahmen umgesetzt worden, um die Widerstandskraft des Finanzsystems zu stärken. Politisches Ziel ist hierbei, so weit wie möglich dafür zu sorgen, dass systemische Krisen verhindert werden oder aber, falls sie eintreten, Haftungsketten so zu gestalten, dass der Steuerzahler möglichst wenig belastet wird. Die Reformen führen zu einer deutlich verbesserten Eigenmittelausstattung, dies gilt sowohl hinsichtlich der Qualität der Eigenmittel als auch der Mindestausstattung. Dieser Teilaspekt betrifft vorrangig die Säule I im Sinne des Baseler Accords.

Bild einer Festungsanlage

Auch in der Säule II sind signifikante Veränderungen zu verzeichnen: In Deutschland hat die Novelle der Mindestanforderungen an das Risikomanagement (MaRisk) einige neue Verpflichtungen für die Unternehmen geschaffen, im europäischen Kontext wird hierbei das Konzept der „Three Lines of Defense" als ein Kernstück der neuen Regulierung gesehen.

Die Assoziation an sportliche und militärische Begriffe ist dabei durchaus gewollt.[1] Hinter dem Bild einer Festungsanlage, die über verschiedene Verteidigungsringe verfügt, um den Kernbereich zu schützen, verbergen sich aus der Perspektive einer regulatorischen Konzeption mehrere Aspekte, die kurz angesprochen und bewertet werden sollen. Dabei wird unter Konzeption eine wirksame Kombination aus Normen, Institutionen und Prozessen verstanden, die den Schutzzwecken der Bankenaufsicht dient.

Das Modul „Besondere Funktionen" in den MaRisk geht zurück auf die EBA Guidelines on Internal Governance aus dem Jahr 2011.[2] Fast zeitgleich hat auch der Baseler Ausschuss für Bankenaufsicht die Rolle einer Line of Defense – nämlich der Internen Revision in einem Konsultationspapier beschrieben, das im Jahre 2012 final veröffentlicht wurde.[3] Gemeinsam sehen diese Standardsetzer das Thema in Governance – also (guter) Unternehmensführung verortet.[4] Ziel von Governance[5] in diesem Sinne ist, mit Hilfe einer wirksamen Aufsicht die Komplexität zu meistern.

Für den Baseler Ausschuss geht es beim Three-Lines-of-Defense-Modell um das Verhältnis zwischen den operativen organisatorischen Einheiten eines Kreditinstituts, den Risikocontrolling- und Compliance-Funktionen und der Internen Revision, also um Einheiten, die nicht zu den Organen eines Unternehmens – im typisch deutschen Modell des Vorstands und des Aufsichtsrats – gehören.

Verschiedene Abgrenzungsmöglichkeiten

Hierbei können die erste und zweite Verteidigungslinie zum Internen Kontrollsystem zusammengefasst werden, die dritte Verteidigungslinie bildet die Interne Revision.[6] In einer anderen Betrachtungsweise wird auch der Abschlussprüfer zur dritten Verteidigungslinie gerechnet, da hier jedoch eine Beschränkung auf Einheiten innerhalb eines Unternehmens erfolgt, zählt der Jahresabschlussprüfer nicht zu den betrachteten Organisationseinheiten.

Die Geschäftseinheiten sind somit die erste Verteidigungslinie. Sie gehen im Rahmen des Bankgeschäftes Risiken ein und sind verantwortlich für die einzelgeschäftsbezogen Identifizierungen, Beurteilungen und die prozessuale Gestaltung. Die hierfür notwendigen Organisationsrichtlinien[7] werden jedoch nicht vollständig von diesen Einheiten entwickelt, vielmehr wird die schriftlich fixierte Ordnung[8] regelmäßig in anderen organisatorischen Einheiten entwickelt, die für die Funktionstrennung zwischen Markt und Marktfolge, die Einräumung von Limiten, die Risikoprozesse, Arbeitsanweisungen und Ähnliches sorgen.

Die zweite Verteidigungslinie ist durchweg heterogener. Hannemann zählt hierzu Supportfunktionen wie das Risikomanagement, Compliance, Recht, Personal, Finanzen, Organisation und IT.[9] Diese Abgrenzung ist nicht unstrittig, jedenfalls zählen zur zweiten Verteidigungslinie Recht, Personal, Organisation und IT. Die Aufgaben werden als „unterstützend" beschrieben, im Vordergrund der MaRisk steht dabei,

Dr. Harald Lob, Projektleiter „Regulatorische Compliance nach MaRisk", KfW, Frankfurt am Main

Wie ist im Sinne des Baseler Ausschusses das Verhältnis zwischen den operativen organisatorischen Einheiten eines Kreditinstituts, den Risikocontrolling- und Compliance-Funktionen und der Internen Revision zu organisieren? Dieser erst im Lichte der Finanzkrise aufgeworfenen Frage nähert sich der Autor anhand der regulatorischen Vorgaben des Baseler Ausschusses über das Bild von drei Verteidigungslinien, wobei er die beiden ersten zum Internen Kontrollsystem zusammenfasst und die dritte der Internen Revision einräumt. Als Möglichkeiten der Abgrenzung nimmt er nicht nur organisatorische Einheiten, sondern auch Aufgaben in den Blick. Die besondere Kunst sieht er darin, im Rahmen der neuen Anforderungen richtig zu navigieren, das heißt, jederzeit zu wissen, welche Wege existieren, welche Auswirkungen Normenänderungen entfalten, rechtzeitig vor Gefahren gewarnt zu werden und Regeln für ein situationsgerechtes Reagieren zu entwickeln. (Red.)

dass Risiken angemessen identifiziert, bewertet und gesteuert werden. Aus der organisatorischen Verantwortung entstehen dabei auch die Aufbau- und Ablauforganisation, die Strategie und das Hinwirken auf die Implementierung der wesentlichen rechtlichen Regelungen und Vorgaben, deren Nichteinhaltung zu einer Gefährdung des Vermögens des Institutes führen kann.[10)]

Abgrenzung über organisatorische Einheiten und über Aufgaben

Diese unscharfe Abgrenzung erscheint zunächst unproblematisch, es wird jedoch zu einem späteren Zeitpunkt aufgezeigt, dass die Zuordnung besonderer Rollen (Key Function Holder) nur einem Teilbereich dieser Funktionen der zweiten Verteidigungslinie dazu führen kann, dass Komplexitäten nicht verringert, sondern erhöht werden.

Die dritte Verteidigungslinie ist – jedenfalls in hier betrachteten Modell – wieder einfach institutionell abzugrenzen: Sie umfasst die Interne Revision. Zu ihren Aufgaben gehören die Prüfung und Beurteilung der Wirksamkeit und Angemessenheit des Risikomanagements im Sinne der MaRisk. Eine weitere Aufgabe ist die Prüfung und Beurteilung des internen Kontrollsystems – also der zusammengefassten ersten und zweiten Verteidigungslinie. Zur Abgrenzung zwischen den Prüfungs- und Beurteilungsaufgaben der Compliance und der Internen Revision schlägt Hannemann vor, der Compliance eine prozessabhängige Überwachung und der Internen Revision eine prozessunabhängige Prüfung zuzuordnen. Alternativ kann die Rolle der Internen Revision auch darin gesehen werden, nur die zweite Verteidigungslinie zu überprüfen.

Die Abgrenzung wird zudem komplizierter, wenn eine Abgrenzung nicht nur über organisatorische Einheiten stattfindet sondern auch über Aufgaben. Hierbei werden der ersten Linie bereichsinterne Maßnahmen, wie beispielsweise die Einhaltung der Funktionstrennung, die Dokumentation zur sachgerechten Anwendung von Leitlinien oder die Anwendung eines Vier-Augen-Prinzips genannt. Der zweiten Linie werden die Überwachung der und die Kommunikation der wesentlichen Risiken zugewiesen mit einer abgrenzbaren Aufgabenteilung zwischen Compliance[11)] und Risikocontrolling, die dritte Linie übt eine prozessunabhängige Prüfung und Beurteilung der Wirksamkeit und Angemessenheit des Risikomanagements im Sinne der MaRisk aus.

Diese wenigen Ausführungen lassen bereits aufscheinen, wo die zentralen Herausforderungen für die Kreditinstitute liegen werden: Welche Beziehungen bestehen zwischen Verteidigungslinie 1 und 2, 1 und 3 sowie 2 und 3? Gibt es bei den Beziehungen der zweiten Verteidigungslinie innerhalb dieser Linie und zu ihren Partnern besondere Beziehungen einzelner Funktionen und wenn ja, wie sind diese sachgerecht im Rahmen der vorgegebenen Normen ausgestaltbar?

Zunächst ist es notwendig, das Institut so zu erfassen und abzubilden, dass eine Steuerung ähnlich einem Navigationssystem möglich wird: Im Rahmen der neuen Anforderungen richtig zu navigieren heißt, jederzeit zu wissen, welche Wege existieren, welche Auswirkungen Normenänderungen entfalten, rechtzeitig vor Gefahren gewarnt zu werden und Regeln für ein situationsgerechtes Regieren zu entwickeln (Abbildung).[12)]

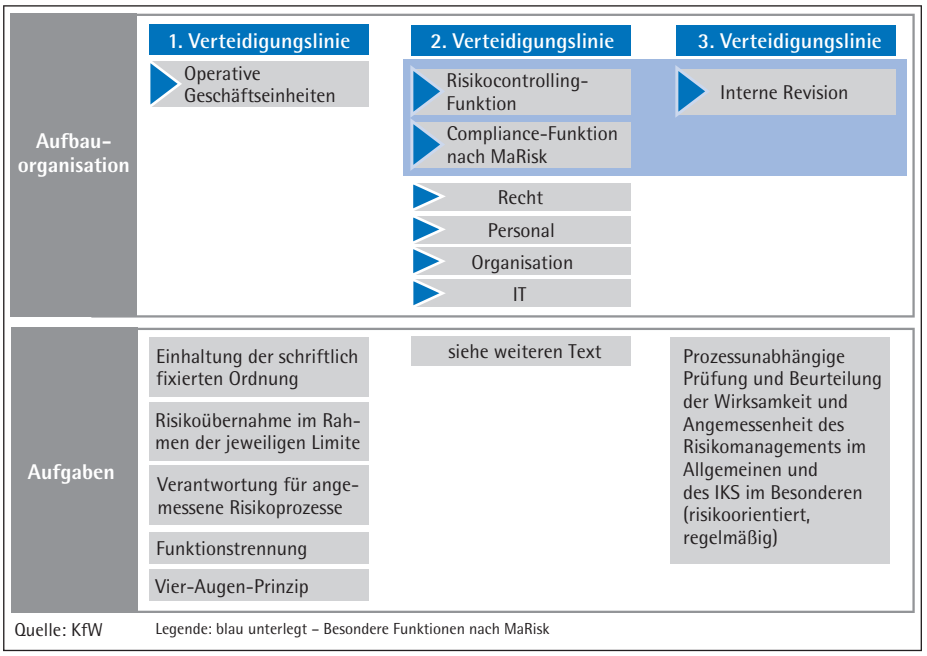
Die Verteidigung von Schutzzwecken: eindeutige Ziele oder Zielkonflikte?

Die soeben beschriebene institutionelle Ausgestaltung gibt nur einen Teilaspekt der Konzeption wieder; ob diese wirksam[13)] ist, kann in einem ersten Schritt anhand der einzuhaltenden Normen beurteilt werden. Die ursprüngliche Zielsetzung bankaufsichtlicher Normen lässt sich zurückführen auf drei Schutzzwecke: Die Vermeidung einer Überschuldung der Bank, von Klumpenrisiken und von Liquiditätsrisiken.[14)] In dieser ursprünglichen Sichtweise war sowohl eine besondere Behandlung des Bankensektors im Vergleich zu anderen Industriesektoren angelegt als auch eine Fokussierung auf eine ausreichende Eigenmittel- und Liquiditätsversorgung, niedergelegt in deutschen Grundsätzen I bis III.

Mit „Basel II" und den entsprechenden KWG-Novellen hat sich der Umfang der Schutzzwecke deutlich erweitert. Neben einer deutlichen Betonung des Verbraucherschutzes wurden im KWG auch die Schutzzwecke Datenschutz und verschiedenen Formen von Compliance-Zielen erfasst. In der Umsetzung von Basel III spielen darüber hinaus Vergütungsfragen eine entscheidende Rolle im Zielsystem, ergänzt um Regelungen zur Sanierung und Abwicklung mit einer entsprechenden Haftungskaskade. Eine deutlichere Betonung erfahren auch Strategie- und Kapitalplanungsprozesse sowie Stresstests.

Mit der Ausweitung der Schutzzwecke ging eine Stärkung der „zweiten Säule" –

Abbildung: Modell zu den drei Verteidigungslinien



Quelle: KfW Legende: blau unterlegt – Besondere Funktionen nach MaRisk

der qualitativen Bankenaufsicht mit ihrer speziellen Ausgestaltung in Deutschland durch die MaRisk – einher. Unabhängig davon, dass die MaRisk in weiten Teilen Ausdruck der Anwendung des Prinzips „Handeln eines ehrbaren Kaufmanns" sind, muss jedoch festgestellt werden, dass die Aufsicht über das Unternehmen sich von der Idee entfernt, dass diese „beinahe als die Zwillingsschwester des Marktes"[15] angesehen werden kann. An die Stelle des Ablauschens des Marktes und der unsichtbaren Hand ist die sichtbare Hand staatlicher Aufsicht getreten. Es ist eine Regelungsdichte entstanden, die praktisch sämtliche Organisationseinheiten des Kreditinstituts betrifft und die die unternehmerische Handlungs- und Entschließungsfreiheit zu mindestens für die Aufbau- und Ablauforganisation auf wenige Handlungsmöglichkeiten beschränkt.

All dies wäre unproblematisch, wenn die Ziele untereinander konfliktfrei wären und die notwendigen Prozesse, so gestaltet werden können, dass ein Prozess dominant ist. Dies ist nicht offensichtlich. Um eine ausführliche Zielkonfliktanalyse zu vermeiden, wird hier als Ausgangshypothese gewählt, dass die Ziele zumindest für die regulatorische Compliance auf eine strategische Variable verengt werden können: Die Vermeidung von Regelungslücken. Damit verengt sich die Diskussion um Zielkonflikte auf eine deutlich geringere Anzahl von strittigen Fällen, nicht gelöst ist damit jedoch ein positiver oder negativer Kompetenzkonflikt zwischen den Akteuren der drei Linien.

Governance, Haftung und Unabhängigkeit

Im dualen System der deutschen Unternehmensverfassung sind als Organe der Vorstand/die Geschäftsführer und ein Aufsichts- oder Verwaltungsrat vorgesehen. Diese Governance ist durch „Beauftragte" ergänzt worden sowie in den neuesten Ausprägungen durch sogenannte Key Function Holder, zu denen die Leiter der Internen Revision, des Risikocontrollings und der Compliance zählen, in der gewählten Begriffsabgrenzung sowohl ausgesuchte Vertreter der zweiten Verteidigungslinie als auch der Vertreter der dritten – unternehmensinternen – Verteidigungslinie.

Die Interne Revision ist Teil eines angemessenen und wirksamen internen Überwachungssystems.[16] Mit der Umsetzung der CRD IV und der MaRisk-Novelle sowie den Verankerungen des Trennbankgesetzes im KWG wurde bestimmt, dass die Interne Revision dem Aufsichtsorgan regelmäßig Bericht erstattet und dieses Aufsichtsorgan zu informieren ist, wenn der Leiter/die Leiterin der Internen Revision wechselt. Der Vorsitzende des Aufsichtsorgans hat gegenüber dem Leiter der Internen Revision einen Anspruch auf direkte und damit durch den Vorstand nicht kontrollierte Informationen.

Für die Geschäftsleitung besteht die Pflicht, die Interne Revision hinsichtlich ihrer Personal- und Sachausstattung so aufzubauen und prozessual zu gestalten, dass sie den wandelnden, gesteigerten Anforderungen der Aufsicht genügt.[17] „Dies setzt voraus, dass die Revision kompetent, souverän selbstbewusst und unabhängig agieren kann."[18] Aus dem Kreis dieser Attribute werden im weiteren Vergleich mit den besonderen Funktionen der zweiten Verteidigungslinie nur „unabhängig" vertieft. Das Bankaufsichtsrecht hat mit den EBA Guidelines on Internal Governance[19], weiteren Konsultationspapieren und den MaRisk darüber hinaus die Bestimmung von Key Function Holder[20] vorgesehen.

In der Ausgestaltung der MaRisk aus der Novelle von 2012 sind in AT 4 neben der Internen Revision zwei weitere „besondere Funktionen" genannt: Die Risikocontrolling-Funktion[21] und eine Compliance-Funktion[22], die jedoch einen anderen Aufgabenzuschnitt hat als die traditionelle Compliance-Funktion. Auch beim Wechsel dieser Funktionen ist das Aufsichtsorgan zu informieren[23], die Risikocontrolling-Funktion hat eine Berichtspflicht an die Geschäftsleitung und gegebenenfalls an die Interne Revision[24], die Compliance-Funktion auch an das Aufsichtsorgan[25], und auch die Revision hat in den Beziehungen zum Aufsichtsorgan eine definierte Kommunikationsordnung.[26]

Benennung von Beauftragten

Keine der bislang dargestellten besonderen Funktionen hat Organcharakter. Vielmehr waren diese Funktionen als Linienfunktionen ausgestaltet und haben im Zeitablauf eine höhere funktionale Qualität erhalten. Eine Form, Funktionen im Unternehmen hervorzuheben, ist die Benennung von Beauftragten, beispielsweise Geldwäsche-, Datenschutz- oder Gleichstellungsbeauftragte. Die dahinter liegende Philosophie ist, einem gewünschten Ziel eine herausragende Bedeutung dadurch zuzuordnen, dass diese aus der hierarchischen Ordnung des Unternehmens herausgelöst sind und mit einem gewissen Autonomiegrad direkt einem Organ unterstellt werden. Die Abgrenzung zu den herausgehobenen Funktionen nach MaRisk ist nicht harmonisiert mit den Regelungen nach der Institutsvergütungsverordnung, dort wird im Hinblick auf die neu in die Schutzzwecke des Bankaufsichtsrechts gehobene Thematik „Vergütung" ein weiterer abzugrenzender Personenkreis definiert: die „Risk Taker".

Die herausgehobenen Funktionen nach MaRisk stellen die Governance sowohl vor die Aufgabe, angemessene Haftungsregeln zu finden, als auch die Zuverlässigkeit und Eignung sicherzustellen.[27] Ferner sind die Funktionen hinsichtlich des „uneingeschränkten Zugangs zu allen Informationen"[28], die für die Erfüllung der Aufgaben wesentlich sind, auszugestalten. Vertieft soll an dieser Stelle das Thema einer Unabhängigkeit beleuchtet werden. Hierbei fällt es aufgrund der traditionellen deutschen Governance schwer, etwas unabhängig zu denken, das zugleich von seiner hierarchischen Umwelt abhängig ist.[29] Die Idee der Unabhängigkeit ist am weitesten durchdacht in Bezug auf die geldpolitischen Funktionen einer Zentralbank,[30] eingeschränkt auch für anderes staatliches Handeln in der Funktion von Rechnungshöfen, spezieller Wirtschaftsaufsichtsbehörden wie dem Kartellamt[31] und unter denselben Voraussetzungen gegebenenfalls auch für Bankaufsichtsbehörden.

Abwesenheit von Zwang

Unabhängigkeit kann dabei nicht gleichgesetzt werden mit einem Fehlen von Vereinbarungen oder das Fehlen von Regelbindungen, Unabhängigkeit ist zunächst einmal die Abwesenheit von Zwang. Unabhängigkeit in diesem Sinne kann aus vier Aspekten betrachtet werden: institutionell, funktionell, finanziell und personell.

– Eine institutionelle Unabhängigkeit kann dadurch gesichert werden, dass es anderen Stellen des Unternehmens verboten ist, Weisungen zu erteilen; selbst der Versuch der Beeinflussung kann untersagt werden, in weitaus abgespeckter Form wird vorausgesetzt, dass wesentliche Weisungen und

Beschlüsse bekannt zu geben sind.[32] Dies kann als Transparenzvorschrift für eine institutionelle Unabhängigkeit angesehen werden.

– Die funktionelle Unabhängigkeit besteht in der alleinigen Verantwortung für die Wahl der Strategien und Maßnahmen. Eine Einbindung in das strategische Zielsystem des Institutes[33] ist damit nicht ausgeschlossen.

– Die Vergütung als Ausdruck der finanziellen Unabhängigkeit und die hierarchische Einordnung, beispielsweise durch „einer Person auf ausreichend hoher Führungsebene"[34] sind so zu gestalten dass eine Unabhängigkeit von einem verständigen Dritten überprüft werden kann.

– Zur personellen Unabhängigkeit tragen die lange zeitliche Amtszeit oder eine Dauerbeschäftigung sowie deren Schutz vor willkürliche Kündigung und lange Kündigungsfristen bei.[35]

Lösungsvorschläge: Wer verteidigt was?

Aus den dargestellten Abgrenzungen heraus lässt sich widerspruchsfreies Konzept entwickeln, das die von den EBA Guidelines und den MaRisk vorgegebenen Mindestanforderungen so transformiert, dass die zugrunde liegenden Begrifflichkeiten gewahrt bleiben.

Einige Überlegungen zur dritten Verteidigungslinie – der Internen Revision – wurden bereits dargestellt. Diese werden nun um die Compliance-Funktion nach AT 4.4.2 MaRisk ergänzt. Die im Rundschreiben der BaFin 10/2012 (BA) vom 14. Dezember 2012 sowie im Protokoll des MaRisk-Fachgremiums vom 24. April 2013[36] genannten wesentlichen Normen, decken zunächst die Normen der klassischen Compliance ab: die Vorgaben des Wertpapierhandelsgesetzes (WpHG), zur Vermeidung von Geldwäsche und Terrorismusfinanzierung, zur Vermeidung sonstiger strafbarer Handlungen und Vorgaben zum Datenschutz. Hinzu kommen auf dieser Ebene Vorgaben zum Verbraucherschutz.

Wird die Compliance-Funktion nach MaRisk (im Folgenden auch: Regulatorische Compliance) organisatorisch der „klassischen Compliance" zugeordnet[37] so vermischen sich die organisatorischen Zuordnungen zur zweiten Verteidigungslinie (Key Function Holder) mit den beschriebenen Aufgabenzuordnungen. Bei einer bisher originären Zuständigkeit, beispielsweise für Geldwäsche- und Betrugsprävention, Wertpapier- und IT-Compliance ist es erforderlich, neu zu regeln, wie sich ein Hinwirken auf die Implementierung wirksamer Verfahren wesentlicher rechtlicher Regelungen und Vorgaben sowie entsprechender Kontrollen gestalten lässt. In ihren eigenen Zuständigkeiten wird die Compliance insgesamt Verantwortung für eine schriftlich fixierte Ordnung, Aufgabenzuordnungen, Vertretungen und Entscheidungsprinzipien haben müssen. Aus der Compliance-Funktion nach MaRisk folgen auch keine Änderungen hinsichtlich der rechtlich vorgegebenen Kontroll- und Überprüfungshandlungen, der Entwicklung von Schulungskonzepten und der Beratung sowohl der Bereiche der ersten und zweiten Verteidigungslinie als auch der Organe der Gesellschaft. Jedoch wird zu überprüfen sein, ob sich der Datenschutz mit den beschriebenen Aufgaben bündeln lässt.

Anders stellen sich die Aufgaben bei anderen wesentlichen Normen dar. Bei der herausgehobenen Normengruppe „Verbraucherschutz" kann sich die Compliance anderer Funktionen und Stellen, nicht jedoch der Internen Revision bedienen. Für den Verbraucherschutz könnte dies sowohl die erste Verteidigungslinie (zum Beispiel der Vertrieb) als auch die zweite Verteidigungslinie sein. Andere beispielhaft genannte Normen sind hingegen leicht der zweiten Verteidigungslinie zuzurechnen. Arbeitsrecht im Personalbereich, (Einkommens-)Steuerrecht zumeist bei Bilanzen und Steuern.

Informationsrechte garantieren und Kontrollrechte einräumen

Die Pflichten der regulatorischen Compliance nach MaRisk können zusammenfassend so beschrieben werden, dass sie darauf hinzuwirken hat, dass im Institut und gegebenenfalls in der Gruppe alle bankaufsichtlichen Regeln eingehalten werden. Hierzu ist es notwendig, entsprechende Informationsrechte zu garantieren[38] und Kontrollrechte[39] einzuräumen.

Ist die regulatorische Compliance nicht an die andere Kontrolleinheit nach AT 4.4.1 angebunden – was nach dem Proportionalitätsprinzip nur für kleinere Institute angemessen erscheint – so stellt sich die Frage nach Beziehungsgestaltungen in der zweiten Verteidigungslinie. Angesichts der herausgehobenen Stellung als Key Function Holder ist ein Hinwirken in die organisatorischen Bereiche der zweiten Verteidigungslinie ebenso denkbar wie entsprechende Überwachungsfunktionen. Bevor diese Beziehungen im Detail erläutert werden, werden die möglichen Beziehungen zur dritten Verteidigungslinie abgegrenzt:

Wie bereits dargestellt ist eine organisatorische Einheit Interne Revision einschließlich regulatorischer Compliance nicht zulässig. Zulässig sind aber alle Vereinbarungen, Richtlinien und Zeitpläne, die die Unabhängigkeit der Internen Revision im Sinne der oben dargestellten Abgrenzungen nicht infrage stellen. Daher ist es durchaus möglich, dass sich die Interne Revision unabhängig entscheidet, welche Kontroll- und Überwachungsfunktionen sie in der ersten und zweiten Verteidigungslinie wahrnehmen will und dies der regulatorischen Compliance mitteilt, die ihrerseits auch in den Aufgabenbereich der Internen Revision fällt. Unabhängigkeit ist also nicht gleichzusetzen mit dem Fehlen von freiwillig eingegangenen Regelbindungen.

Beziehungen innerhalb der zweiten Verteidigungslinie

Nach dieser Abgrenzung zu der dritten Line of Defense geht es abschließend um die Beziehungen innerhalb der zweiten Verteidigungslinie. Sind einige Bereiche innerhalb dieser Linie gleicher als die Anderen, und welche Komplexitätsreduzierung ist denkbar?

Die Bestimmung der beiden Key Function Holder in der zweiten Verteidigungslinie legt nahe, dass diese sachgerecht ähnlich behandelt werden sollen wie der Key Function Holder der dritten Verteidigungslinie. Die dargestellten besonderen Zugangsrechte zu Informationen, die Transparenzvorschriften zur Sicherung einer Unabhängigkeit und die besonderen Berichtswege legen diese Betrachtungsweise nahe. Diesen Rechten stehen korrespondierende Pflichten gegenüber. Als Mindestanforderung ist bereits in den MaRisk eine Berichtspflicht vorgesehen worden.

Wenn die Verantwortung in weiten Teilen der ersten Vereidigungslinie zugeordnet

wird, so ist es nicht verwunderlich, dass dort erhebliche Investitionen vorgenommen werden, um dieser Verantwortung gerecht zu werden. Sollen in Zeiten angespannter Kosten- und Ertragssituationen diese Investitionen effizient erfolgen, so setzt dies voraus, dass die zweite und dritte Verteidigungslinie ihre Wertvorstellungen und Planungs- und Prüfungshypothesen schnell und eindeutig formulieren. Im Interesse des Instituts ist dazu auch das „Navigationssystem" nachvollziehbar so zu entwickeln, dass die verschiedenen Anforderungen kosteneffizient erfüllt werden. So kann sichergestellt werden, dass sich die erste Verteidigungslinie nicht nur als Lieferant des Grüne-Ampeln-Status für die anderen Linien sieht.

Hierzu gehört als Verantwortung der zweiten Verteidigungslinie beispielsweise die zumindest zeitliche Zusammenfassung der Risikoanalysen, -inventuren und Gefährdungsanalysen, mit denen die operativen Einheiten sich zu beschäftigen haben, sowie die die Entwicklung einer einheitlichen Nomenklatur für die neu eingeführten Begrifflichkeiten.

Reziprozität

Die Ausgestaltung der Beziehungen innerhalb der zweiten Linie – insbesondere zwischen den beiden Key Function Holder – sollte von Reziprozität gekennzeichnet sein. So wie die regulatorische Compliance Rechte gegenüber dem Risikocontrolling hat, so gilt dies auch umgekehrt. Ist im Risikocontrolling beispielsweise die Steuerung von operationellen Risiken zugeordnet, so wird auch die regulatorische Compliance von dieser Systematik erfasst.

Der Umweg über eine strategische Variable,[40] abgeleitet aus dem Unternehmensinteresse, erweist sich dabei als wertvoll. Er reduziert nicht nur die Diskussion um potenzielle Zielkonflikte auf tatsächliche, sondern leistet auch eine Reduzierung der Komplexität durch den Ausschluss von Beliebigkeiten ohne zu einer Lösung „There ist no alternative" zu kommen. Durch die Vermeidung verschwommener Abgrenzungen zwischen den drei Linien und die vorgeschlagene Rollenverteilung ist das lösungspotenzial überschaubarer und im Navigationssystem erfassbar geworden.

Die so beschriebene Konzeption macht es auch leichter, über die Fragen nach der Angemessenheit der regulatorischen Anforderungen zu diskutieren. Bei der vorgeschlagenen Vorgehensweise geht es gerade nicht um einen Gegensatz zu viel – zu wenig, sondern den Ausschluss von Normen, Institutionen und Prozessen, die nicht konzeptionskonform sind.[41]

Diese ersten Überlegungen reichen aus, die neuen Regulierungsideen in ersten Schritten sachgerecht umzusetzen. In der Sprache eines der erwähnten Spiele und der Aufgaben der Verteidigung heißt das: „Die Null steht". Dies reicht aus, um nicht auf einem Abstiegsplatz zu stehen, dies reicht jedoch nicht aus, um der Champions League mitzuspielen.

Eine Kultur der Integrität schaffen

Hierzu sind weitere Aspekte auf der Basis der dargestellten Verteidigungslinien und des Navigationssystems auszubauen. Ziel ist dabei nicht nur das Vermeiden von Fehlern, sondern vielmehr das Sicherstellen einer Kultur der Integrität. Letztlich geht es um den Erhalt des Geschäftsmodells und seiner sachgerechten innovativen Weiterentwicklung. Hierzu muss die Compliance-Funktion glaubhaft ihre Beraterrolle ausfüllen können. Sie braucht dazu nicht nur, wie in den MaRisk formuliert, rechtliche Absicherungen, sondern zusätzlich das Vertrauen aller Partner im Unternehmen.

Für Hinweise zu einer früheren längeren Fassung dankt der Autor seinen Kollegen in der KfW Compliance und der externen Unterstützung durch Mitarbeiter von KPMG AG WPG. Verbleibende Fehler und Irrtümer gehen ausschließlich zulasten des Autors, der in diesem Beitrag ausschließlich seine persönliche Auffassung wiedergibt.

Fußnoten

[1] Es kann beispielsweise an strategische Spiele (wie Schach) oder Mannschaftsspiele (zum Beispiel Fußball) gedacht werden. In jedem Fall ist dabei immer eine Angriffsfunktion mitzudenken, die hier nur aus Platzgründen nicht ausführlich behandelt wird.

[2] European Banking Authority: EBA Guidelines on Internal Governance, 27. September 2011.

[3] Vgl. Basel Committee on Banking Supervision, The Internal Audit Function in Banks, November 2011 und Juni 2012.

[4] Vgl. dazu Malik, Fredmund, Die richtige Corporate Governance, Frankfurt am Main 2008.

[5] Vgl. zu einer längeren Herleitung der Governance-Überlegungen: Lob, Harald, Überwachung und Regulierung der KfW: Status quo und Perspektiven, in: Morner, Michèle (Hrsg.); 1. Speyerer Tagung zu Public Corporate Governance, Speyerer Arbeitsheft Nr. 213, Speyer 2014, S. 150 bis 165.

[6] So Hannemann, Ralf et al., Mindestanforderungen an das Risikomanagement, 4. Auflage, Stuttgart 2013, S. 371.

[7] Vgl. dazu MaRisk AT5.

[8] § 25 a, Abs. 1 Ziffer 4 KWG.

[9] Hannemann, Ralf et al., a.a.O., S. 370.

[10] MaRisk, AT 4.4.2 Tz. 2.

[11] Der Compliance-Funktion nach MaRisk obliegt dabei die Überwachung des und die Kommunikation zu dem Risiko, das sich aus der Nichteinhaltung gesetzlicher und regulatorischer Vorgaben ergeben kann.

[12] So schon Malik, Fredmund, Strategie, Frankfurt am Main 2011, S. 36.

[13] Wirksam ist dabei ein Begriff, den sowohl Malik, Die richtige Corporate Governance a.a.O., als auch die MaRisk verwenden, in wirtschaftspolitischen Konzeptionen wird der Begriff beispielsweise beim Konzept eines wirksamen Wettbewerbs verwendet, vgl. dazu Schmidt, Ingo, Wettbewerbspolitik und Kartellrecht, 8. Auflage, Stuttgart 2005, S. 10 f.

[14] Diese Darstellung folgt einem gemeinsam mit PwC entwickelten Schulungskonzept.

[15] So Malik, a.a.O, S. 121.

[16] Vgl. § 25 a KWG.

[17] Vgl. Wiesemann, Bernd, Interne Revision, Erwartungen der Bankenaufsicht, in: BaFin Journal März 2014, S. 20.

[18] Ebenda.

[19] European Banking Authority: EBA Guidelines on Internal Governance, 27. September 2011.

[20] European Banking Authority: EBA Cunsultation Paper on draft Guidelines for assessing the suitability of members of the management body and key function holders of a credit institutions, 18. April 2012.

[21] AT 4.4.1 MaRisk.

[22] AT 4.4.2 MaRisk.

[23] AT 4.4.1. Ziffer 5, und AT 4.4.2 Ziffer 7 MaRisk.

[24] AT 4.4.1, Ziffer 2, letzter Spiegelstrich MaRisk.

[25] AT 4.4.2, Ziffer 5 MaRisk.

[26] Vgl. hierzu abwägend Hannemann, Ralf et al., a.a.O:, S. 424 f.

[27] Hierfür geben die Versicherungsmöglichkeiten für Organe (D&O-Versicherung) sowie die Zuverlässigkeit und Eignungs-/Sachkundeprüfungen gute Anhaltspunkte, sodass diese Aspekte hier nicht weiter vertieft werden.

[28] Beispielhaft At 4.4.2 Ziffer 5 MaRisk.

[29] Vgl. dazu grundsätzlicher Baecker, Dirk, Neurosoziologie. Ein Versuch, Frankfurt 2014, S. 47.

[30] Die folgenden Beispiele und Abgrenzungen sind diesem Bereich entnommen.

[31] Vgl. Baum, Thomas, Per se Rule versus Rule of Reason und Kartellamtsautonomie: Eine Hypothese auf der Basis der Public Choice-Theorie, in: Wirtschaft und Wettbewerb 32 (1982), S. 912 ff.

[32] Vgl. AT 4.4.2 Ziffer 5 MaRisk.

[33] Vgl. AT 4.2 MaRisk.

[34] So in AT 4.4.1, Ziffer 4 MaRisk.

[35] Ein entsprechender Schutz ist beispielsweise für den Vergütungsbeauftragten nach der Institutsvergütungsverordnung vorgesehen.

[36] Vgl. Hannemann, Ralf et al., a.a.O.; S. 1293 ff. und S. 1356 ff. (im Folgenden: Protokoll).

[37] Protokoll, zitiert nach Hannemann, Ralf et al., a.a.O., S. 1359 (Organisatorische Einbindung).

[38] AT 4.4.2, Ziffer 5 MaRisk.

[39] AT 4.4.2, Ziffer 1, Satz 2 MaRisk.

[40] Aus Platzgründen wurde dieser Aspekt stark gekürzt, eine Herleitung findet sich bei Lob, Harald, Die Entwicklung der französischen Wettbewerbspolitik, Frankfurt am Main 1987, S. 22 ff.

[41] Vgl. beispielhaft Elliott, Douglas C., Radical Regulatory Action Would Do More Harm Than Good, in Safe Newsletter 1/2014, S. 14 als Plädoyer für eine „step by step" Implementierung.