Holger Kahl / Oliver Kozica / Tom Martens / Ralf B. Schlemminger

Effiziente Weiterentwicklung der **MaRisk-Compliance-Funktion**: Herausforderungen projektorientiert meistern

Der Begriff Compliance steht für die Einhaltung rechtlicher Regelung und Vorgaben.[1] Für alle Unternehmen ist dies ein bedeutsames Thema, zumal schwarze Schafe bei der Rechtsverfolgung – leider zu Unrecht – ganze Branchen in Misskredit bringen können. Bei Verletzungen von Rechtsnormen drohen den Unternehmen nicht nur kurzfristige Geldbußen, Strafen oder Schadensersatzzahlungen, sondern auch längerfristige Reputationsschäden. Dauerhafter Erfolg wird sich allerdings nur dann einstellen, wenn sich ihre Kunden darauf verlassen können, dass geltende Rechtsnormen befolgt werden.

Verschärfung der Compliance-Anforderungen

In der Kreditwirtschaft hat die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) mit ihrer Novellierung der Mindestanforderungen an das Risikomanagement (MaRisk) im Dezember 2012 die Anforderungen an die Compliance-Strukturen von Banken verschärft.[2] Nach den MaRisk bildet die Compliance-Funktion zusammen mit dem Risikocontrolling und der Revision die funktionalen Säulen des Risikomanagements (Abbildung 1). In diesem System hat die MaRisk-Compliance-Funktion die Rechtsnorm-Einhaltung durch die Geschäfts- oder Fachbereiche zu überwachen und präventiv auf die Implementierung wirksamer Verfahren[3] zu deren Einhaltung hinzuwirken. So soll das Compliance-Risiko mit den schon genannten monetären beziehungsweise imagebezogenen Auswirkungen eingedämmt werden. Damit unterstützt die Compliance-Funktion einerseits den Vorstand in seiner Gesamtverantwortung und andererseits die Abteilungen (und vorhandene Verbundunternehmen), die als „erste Verteidigungslinie"[4] für die Rechtsnormkonformität uneingeschränkt verantwortlich sind.

Durch die MaRisk-Novelle ist der Compliance-Fokus deutlich erweitert worden: Neben den bereits vorhandenen Verfahren zur Vermeidung von Verstößen gegen die Vorgaben zu Wertpapierdienstleistungen (WpHG-Compliance) oder zur Bekämpfung von Geldwäsche, Terrorismusfinanzierung und sonstigen strafbaren Handlungen (Zentrale Stelle) sind neuerdings alle Verfahren zur Einhaltung der für ein Institut wesentlichen Rechtsnormen zu überwachen.

Weiterentwicklung im Spannungsfeld

Die Weiterentwicklung der Compliance-Startorganisation – gemäß den MaRisk hätte diese bis spätestens Ende 2013 grundsätzlich stehen müssen – ist nicht leicht zu gestalten.[5] Die Institute betreten hier immer noch Neuland; Best-Practice-Lösungen zu den teilweise nicht eindeutigen Anforderungen sind noch in der Entwicklung. Vor diesem Hintergrund wäre es nahe liegend, Konzepte aufzustellen, die im Zweifel Lösungen mit „Gürtel und zusätzlichen Hosenträgern" vorsehen, um auch den engsten Auslegungen der Anforderungen gerecht zu werden und mögliche strafrechtliche Konsequenzen bei Defiziten zu vermeiden.[6] Dies kann jedoch gegen das Effizienzgebot verstoßen, dem auch die Compliance-Funktion genügen muss. Ohne Frage zeichnet sich hier ein Spannungsfeld ab. Dieser Artikel skizziert Ansätze, wie Kreditinstitute in Projekten zur Compliance-Weiterentwicklung strukturiert praxisorientierte Lösungen finden können, die diesen polarisierenden Ansprüchen gerecht werden.[7]

Holger Kahl, interner Revisor, Oliver Kozica, Organisation und Informationstechnologie, Dr. Ralf B. Schlemminger, Senior Inhouse-Consultant/Organisation und Informationstechnologie, alle Die Sparkasse Bremen AG, und Tom Martens, externer Berater (Compliance)

Die deutsche Bankenaufsicht hat mit der vierten MaRisk-Novelle die Compliance-Anforderungen deutlich erweitert. Und die Institute haben aus Sicht der Autoren schon mit der ersten Umsetzungswelle bis Ende 2013 Neuland betreten und entwickeln weiterhin Best-Practice-Lösungen. Um auch den engsten Anforderungsauslegungen gerecht zu werden, so die Bestandsaufnahme der Autoren, sind im Zweifel teure, „konservative" Strukturen geschaffen worden. Dies sehen sie jedoch nicht unbedingt mit dem Effizienzgebot im Einklang, dem auch die Compliance-Funktion gerecht werden muss. Sie verdeutlicht Ansätze, wie Kreditinstitute in Weiterentwicklungsprojekten strukturiert praxisorientierte Lösungen finden können, die diesen polarisierenden Ansprüchen gerecht werden. (Red.)

Strukturierung der Weiterentwicklungsaufgaben

„Aller Anfang ist schwer!", lautet ein deutsches Sprichwort. Eine Systematisierung anstehender Aufgaben mithilfe eines sogenannten Projektstrukturplans kann hier zu deutlichen Einstiegserleichterungen führen. Auch wenn die Baustellen von Institut zu Institut verschieden sein werden, lässt sich doch ein Kanon von neun „klassischen" Aufgaben bei der MaRisk-Compliance-Weiterentwicklung erkennen. Dieser Strukturplan über die Aufgaben (Abbildung 2) ist ohne Frage Dreh- und Angelpunkt für die Einschätzung des Weiterentwicklungsbedarfs, des Bedarfs an internen und gegebenenfalls externen Fachkräften sowie des Umsetzungsaufwands.

Im Folgenden sollen die Gegenstände der ersten sechs Arbeitspakete näher beschrieben und mögliche Arbeitsergebnisse unter

Darlegung zentraler Herleitungsargumente aufgezeigt werden.

Anforderungsanalyse:
Das A und O zum Projektstart

Im ersten Arbeitspaket „Analyse der Anforderungen" steht die Beschäftigung mit den aufsichtlichen Anforderungen an. Drei aufsichtliche Werke stehen im Fokus (Abbildung 3), in denen allgemeine und spezielle MaRisk-Compliance-Anforderungen aufgeführt sind. Ergänzend sind das Protokoll des BaFin-Fachgremiums sowie gegebenenfalls die EBA-Richtlinien zur guten Unternehmensführung heranzuziehen.[8] In der Projektarbeit hat es sich bewährt, auch einen Blick auf die Anforderungen des Instituts der Wirtschaftsprüfer (IDW) an eine Compliance-Organisation – abgeleitet aus deren Prüfungsstandards – zu werfen.[9]

Die Analysearbeit hat insofern einen hohen Stellenwert, als die Freiheitsgrade bei Konzept und Umsetzung herausgearbeitet werden müssen (Öffnungsklauseln). Nur so kann die Balance zwischen aufsichtlich geforderten und effizienten Lösungen gefunden werden. Diese Arbeit ist nicht leicht, da in der laufenden Diskussion durchaus der ein oder andere Compliance-Experte zu finden ist, der bei der Anforderungsexegese „päpstlicher als der Papst" sein möchte.

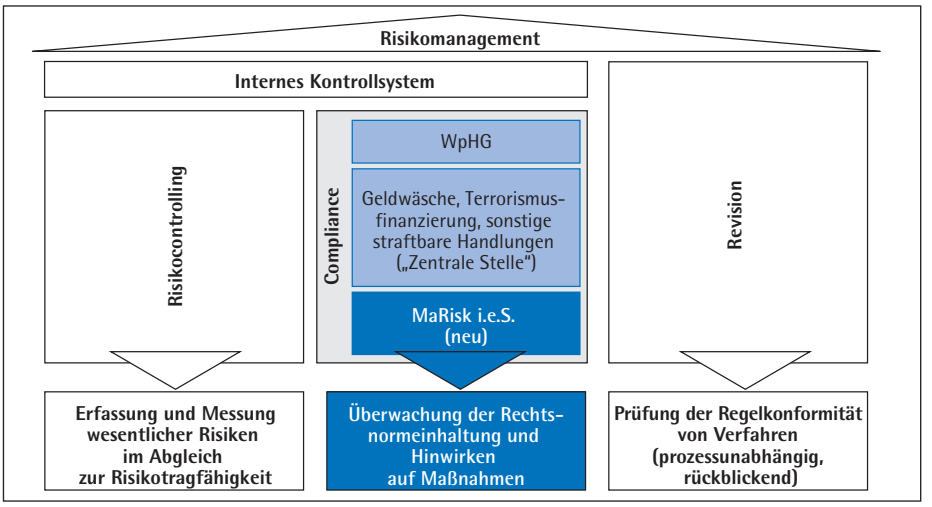
Neben den Freiheitsgraden sollte die Analyse auch die nicht eindeutigen MaRisk-Anforderungen herausstellen (Anforderungsunschärfen). Hier lohnt es sich, insbesondere die betriebswirtschaftliche Diskussion zu verfolgen oder – im Falle einer Verbandsorganisation – deren Empfehlungen und Leitfäden mitzuverarbeiten.

Abschluss der Anforderungsanalyse sollte die Zuordnung einzelner Anforderungspositionen auf die Arbeitspakete des Projektstrukturplans sein, um eine zielgerichtete Projektarbeit zu gewährleisten. Die Anforderungsliste insgesamt stellt auch eine Checkliste zur Bewertung finaler Projektergebnisse dar (Abbildung 3).

Rahmenziele festlegen

Es ist sinnvoll, im zweiten Arbeitspaket die Rahmenziele oder Compliance-Grundsätze festzulegen und so Orientierung für alle Beteiligten zu geben. Die MaRisk bieten hier zwei besondere Anknüpfungspunkte

Abbildung 1: Säulen des Risikomanagements



für Festlegungen. Erster Anknüpfungspunkt ist die Forderung der Aufsicht nach einem „Hinwirken" der MaRisk-Compliance-Funktion auf die Implementierung wirksamer Verfahren zur Rechtsnormeinhaltung und Kontrolle.[10] Institutsspezifisch ist die Entscheidung zu fällen, ob die Fachbereiche eher „an einer kurzen oder langen Leine" geführt werden sollen (Abbildung 4).

Effizienzgründe sprechen dafür, den „Schieberregel" beim Rahmenziele-Spektrum so einzustellen,[11] dass nur minimale Vorgaben gemacht werden, wie zum Beispiel die Verwendung von Standardverträgen im Kundenverkehr. Ansonsten sollte sich die Compliance-Funktion auf die Verfahrensüberwachung und den Hinweis auf die Abstellung festgestellter Verfahrensdefizite beschränken. Gegen eine mögliche Zielfixierung am anderen Ende der Gestaltungsskala – in jedem Auswahl- und Entscheidungsprozess von Verfahren eingebunden zu sein – sprechen nicht nur der hohe Aufwand, sondern auch die schon zitierte Verantwortungszuweisung an die Fachbereiche im Modell der drei Verteidigungslinien. Bei allzu starker Einbindung ist zudem die grundsätzliche Gefahr zu bedenken, dass dies den Blick für eine unbefangene „neutrale" Bewertung der Verfahren trüben kann.

Der zweite Anknüpfungspunkt ist die MaRisk-Anforderung an eine „Identifizierung der wesentlichen rechtlichen Regelungen und Vorgaben, deren Nichteinhaltung zur einer Gefährdung des Vermögens des Instituts führen kann, ... unter Berück-

Abbildung 2: Muster-Projektstrukturplan

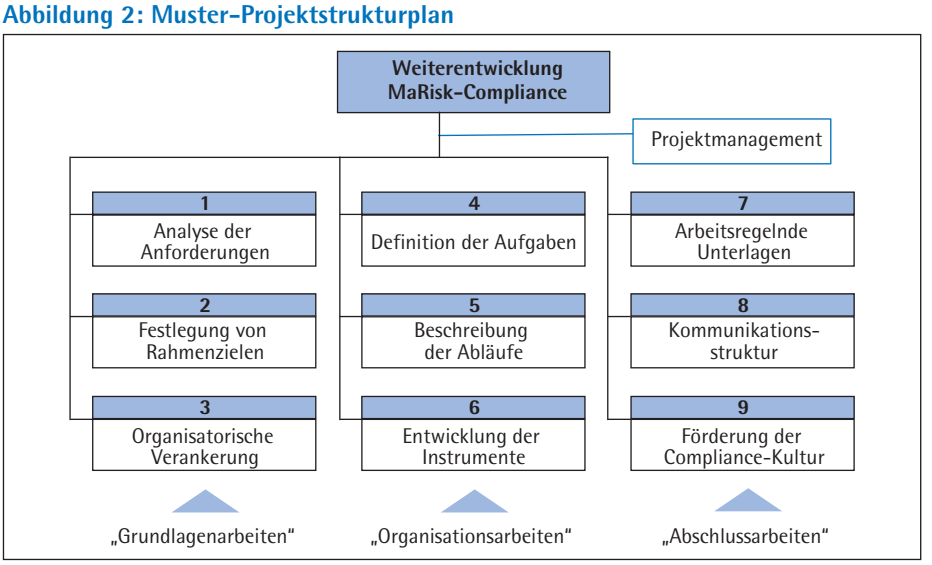


Abbildung 3: Allgemeine und spezielle MaRisk-Compliance-Anforderungen

				Abschluss-Check
Aufsichtliche Anforderungen	Allgemein	Art. 321 EU-Richtlinie (CRR)	Verfahren zur Gewährleistung der Rechtsbefolgung (Compliance)	☐ ok ☐ nok
			Grundsätze für die Behandlung von Verstößen	☐ ok ☐ nok
		§ 25a KWG	Risikomanagement mit IKS, bestehend aus Compliance- und Risikocontrolling-Funktion, sowie Revision	☐ ok ☐ nok
			IKS mit aufbau- und ablauforganisatorischen Regelungen und Abgrenzung der Veranwortungsbereiche	☐ ok ☐ nok
			IKS mit Prozessen zur Identifizierung, Beurteilung, Steuerung und Überwachung von Risiken	☐ ok ☐ nok
			Angemessene und technischorganisatorische Ausstattung	☐ ok ☐ nok
	Speziell	AT 4.4.2 MaRisk	Compliance-Funktion zum „Entgegenwirken" der Compliance-Risiken	☐ ok ☐ nok
			Hinwirken dieser Funktion auf wirksame Verfahren und Kontrollen	☐ ok ☐ nok
			Unterstützung und Beratung der Geschäftsleitung durch diese Funktion	☐ ok ☐ nok
			Regelmäßige Identifizierung wesentlicher rechtlicher Regelungen und Vorgaben durch diese Funktion	☐ ok ☐ nok
			Unmittelbare Unterstellung der Funktion unter der Geschäftsleitung mit Berichtspflicht	☐ ok ☐ nok
			Rückgriffsmöglichkeit dieser Funktion auf andere Funktionen	☐ ok ☐ nok
			Benennung eines Compliance-Beauftragten	☐ ok ☐ nok
			Ausreichende Befugnisse und uneingeschränkte Informationszugänge für die Mitarbeiter dieser Funktion	☐ ok ☐ nok
			Bekanntgabe von Weisungen und Beschlüsse der Geschäftsleitung an diese Funktion	☐ ok ☐ nok
			Rechtzeitige Informationen über bestimmte Regelungsänderungen an die Mitarbeiter dieser Funktionen	☐ ok ☐ nok
			Jährliche und anlassbezogene Berichterstattung an Geschäftsleitung, Aufsichtsrat und interne Revision	☐ ok ☐ nok
			Information an den Aufsichtsrat bei Wechsel des Compliance-Beauftragten	☐ ok ☐ nok
Prüfungspraxis	Allgemein	IDW PS 980	Compliance-Kultur, geprägt durch Management und Aufsichtsorgan („tone at the top")	☐ ok ☐ nok
			Festlegung der Ziele, die mit dem Compliance-Management-System (CMS) erreicht werden sollen, durch gesetzliche Vertreter	☐ ok ☐ nok
			Festlegung von CMS-Rollen, Verantwortlichkeiten (Aufgaben), Aufbau-/Ablauforganisation durch das Management	☐ ok ☐ nok
			Feststellung der Compliance-Risiken mit einem Verfahren zur Risikoerkennung und -berichterstattung	☐ ok ☐ nok
			Analyse festgestellter Risiken im Hinblick auf Eintrittswahrscheinlichkeit und Folgen (zum Beispiel Schadenshöhen)	☐ ok ☐ nok
			Einführung von Grundsätzen und Maßnahmen zur Begrenzung von Compliance-Risiken (Compliance-Programm)	☐ ok ☐ nok
			Kommunikation von Compliance-Programm, Rollen und Verantwortlichkeiten sowie Berichtswegen bei Regelverstößen	☐ ok ☐ nok
			Überwachung der Angemessenheit und Wirksamkeit des CMS mit entsprechender Berichterstattung	☐ ok ☐ nok

sichtigung von Risikogesichtspunkten".[12] Hier zeigt sich das Effizienzkalkül der Aufseher, dass nicht jede geringfügige Vermögensgefährdung unbedingt durch Verfahren „mit Netz und doppeltem Boden" unter Vernachlässigung jeglicher Kosten auszuschließen ist. Vielmehr hat jedes Institut eine Risikoschwelle zu definieren, die die unwesentlichen von den wesentlichen Compliance-Risiken, also Gefährdungspotenzialen durch Nichteinhaltung, trennt.

Risikoschwelle mittels Risikodiagramm festlegen

Eine solche Schwellendefinition ist beileibe kein Hexenwerk. Risikomanagementtheorie und -praxis sehen hier eine Bewertung vorgefundener „Rechtsnormeinhaltungsschwächen" in bestimmten Bereichen sowohl nach der Risikodimension „Eintrittswahrscheinlichkeit" (einer Rechtsnormverletzung) als auch der Dimension „Risikoausmaß" (Schadenshöhe im Falle einer Verletzung).[13] So wird ein Risikodiagramm aufgefächert, in dem dann eine Schwelle – entweder in Form einer Geraden oder einer Treppenstufe – zu legen ist (Abbildung 5). Die konkrete Lage ist institutsindividuell nach der Risikotragfähigkeit (dem Risikokapital) im Zusammenhang mit der Risikosituation zu bestimmen. Diese Bestimmung kann allerdings nicht in der Verantwortung der Compliance-Funktion alleine liegen, sondern ist aufgrund der Tragweite für die Gesamtbanksteuerung federführend vom Risikocontrolling vorzubereiten und vom Bankvorstand zu entscheiden.

Eine einmal gefundene organisatorische Verankerung der MaRisk-Compliance-Funktion ist nicht auf alle Ewigkeit „fest zementiert". Im Falle einer nicht zentralen Compliance-Einheit, die alle Compliance-Funktionen vereint, macht die Aufnahme des dritten Arbeitspaketes in einem Weiterentwicklungsprojekt Sinn, um die Angemessenheit der Verankerung zu überprüfen. Möglicherweise ergeben sich in Anbetracht gleicher oder ähnlicher Arbeiten der WpHG-Compliance und der zentralen Stellen – wie zum Beispiel die Durchführung von Gefährdungsanalysen oder die Erstellung von Compliance-Berichten – durch eine Zusammenfassung Synergie- und Effizienzeffekte. Die unmittelbare Unterstellung der MaRisk-Compliance-Funktion unter der Geschäftsleitung darf allerdings nicht angetastet werden.[14]

Das vierte Arbeitspaket umfasst die Überprüfung und gegebenenfalls Neufestlegung der Aufgaben der MaRisk-Compliance-Funktion. Sie lassen sich – ähnlich wie die der bereits seit langem eingeführten WpHG-Compliance- oder der Zentralen-Stelle-Funktion – mit „Überwachung", „Beratung" und „Koordination" umschreiben. Die grobe Abfolge der Aufgaben bildet im Kern einen (Steuerungs-)Regelkreis; die klassischen vier Risikomanagementaufgaben Risikoidentifikation, -bewertung, -steuerung und „-überwachung" sind hierbei nicht zu übersehen. Wie in Abbildung 6 exemplarisch dargestellt, können diese Aufgaben weiter in Einzelaufgaben zerlegt werden.

Compliance-Organisation

Die Gretchenfrage ist nun die nach Art und Umfang der Beteiligung der MaRisk-Compliance-Funktion beziehungsweise der Geschäfts- oder Fachbereiche. Dies hängt von der Festlegung der Rahmenziele ab und sollte durch eine entsprechende Kennzeichnung bei den Aufgabenträgern deutlich gemacht werden.

In bestimmten Situationen kann es hierzu sinnvoll sein, den detaillierten Ablauf in sogenannten Prozessdiagrammen zu beschreiben. Ein solches zweidimensionales

Instrument führt in der einen Dimension alle Aufgaben auf und in der zweiten die beteiligten Einheiten, sodass die Abfolge der Aufgaben quasi „als Prozesszug" durch die Einheiten sichtbar wird. Dieses Instrument hilft nicht nur den effizientesten Aufgabenfluss im Rahmen der Konzeption zu finden, sondern auch Verantwortungsklarheit und die Chance auf eine nachhaltige Etablierung des Standardprozesses in der Praxis zu erhöhen.

Compliance-Instrumente zur effizienten Aufgabenerledigung

Es ist eine Binsenweisheit, dass Aufgaben nur dann effizient erledigt werden können, wenn Instrumente zur Verfügung stehen, die sowohl wirksam als auch einfach zu handhaben sind. In der Diskussion über die MaRisk-Compliance-Ausgestaltung werden mehrere Instrumente genannt, auf das Rechtsnorm-Inventar und die Gefährdungsanalyse wird im Folgenden näher eingegangen.

Rechtsnorm-Inventar: Die Aufstellung eines Rechtsnorm-Inventars für ein Kreditinstitut ist zwar aufsichtsrechtlich nicht explizit gefordert, für einen effektiven Überwachungsprozess durch die MaRisk-Compliance-Funktion jedoch zu empfehlen. Ein solches Inventar ist eine geordnete Sammlung aller rechtsform- und geschäftsmodellrelevanten Rechtsnormen einer Bank. Diese Rechtsnormen werden entweder Produkten, Organisationseinheiten oder Geschäftsprozessen zugeordnet. Für letztere Zuordnungslogik spricht die in der Praxis vorzufindende Sicht, ein Kreditinstitut als ein Gebilde abzählbarer, kategorisierter Geschäftsprozesse mit eindeutigen Prozessverantwortlichen darzustellen.

Bei der Architektur eines solchen Rechtsnorm-Inventars ist auf Übersichtlichkeit und leichte Pflege zu achten. Deshalb sollten in der Überblicksansicht die Rechtsnormen zu Blöcken zusammengefasst werden, sogenannten Rechtsnorm-Clustern, die wiederum den definierten Prozessen in einem Institut zugeordnet wurden. In Detailansichten werden pro Cluster die einzelnen Rechtsnormen aufgeführt. Eine solche Architektur ist nicht statisch, sondern dynamisch: Wenn Rechtsnormen eingeführt oder verändert werden, ist es die Aufgabe der jeweiligen Prozessverantwortlichen aus den Fachbereichen, den oder die Prozess(e) hinsichtlich der veränderten Rechtslage zu überprüfen. Besteht ein Handlungsbedarf, hat eine entsprechende Anpassungsmeldung an die MaRisk-Compliance-Funktion zu erfolgen, aus der hervorgeht, bis wann und in welcher Form die Prozessanpassung erfolgt.[15]

Die MaRisk-Compliance-Funktion muss grundsätzlich die rechtsnormrelevanten Veröffentlichungen im Blick halten und kann anhand des Inventars relativ einfach die Prozessverantwortlichen ausmachen, von denen eine entsprechende Meldung eigentlich kommen müsste. Die Kontrolle darüber, ob und wie die Meldung erfolgt und welche Maßnahmen zum vermeintlichen Defizitabbau ergriffen werden, ist gut durchführbar. Zugleich wird ein wichtiger Impuls zur Aktualisierung des Inventars gegeben. Dank dieser Verfahrensweise ist es möglich, zwei Fliegen mit einer Klappe zu schlagen: laufende Rechtsnormänderungs-Überwachung und Aktualisierung des Inventars. Last, but not least ist ein Rechtsnorminventar auch die zentrale Grundlage zur Festlegung der Stichprobe für die Gefährdungsanalyse, die nachfolgend beschrieben wird.

Gefährdungsanalyse: Die erhebliche Aufgabenerweiterung der Compliance-Funktion durch die vierte MaRisk-Novelle wirft die Frage nach einem effizienten Analyse- und Bewertungsinstrument auf, um zielgerichtet die Gefährdungslage bei der Rechtsnormeinhaltung zu ermitteln und damit die wesentlichen Compliance-Risiken zu identifizieren. Die hierfür benötigte Wesentlich-

Abbildung 4: Rahmenziele-Spektrum der MaRisk-Compliance

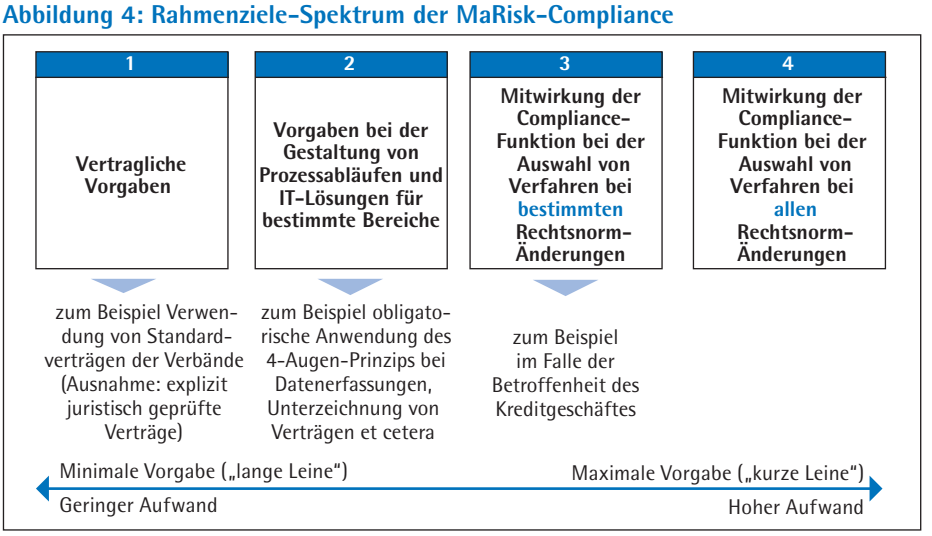
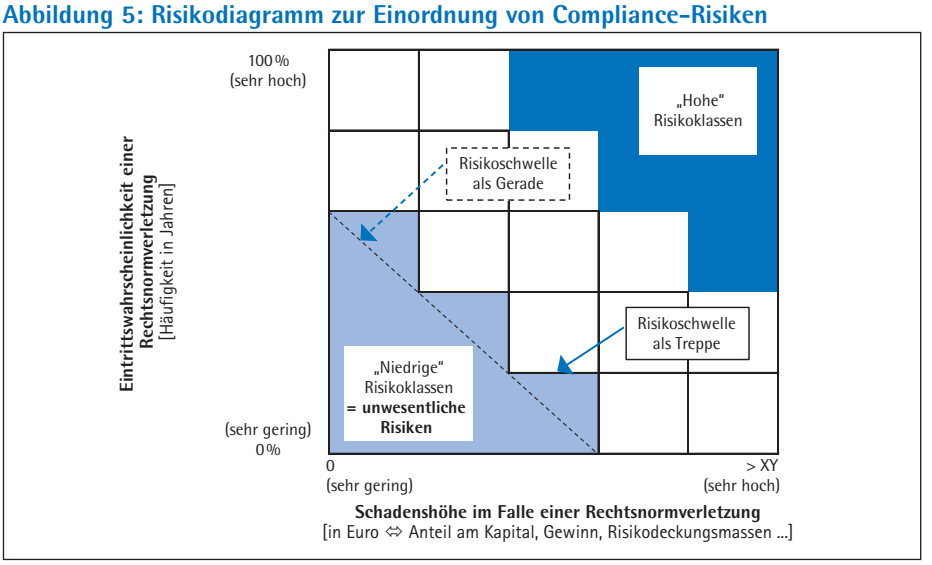


Abbildung 5: Risikodiagramm zur Einordnung von Compliance-Risiken



keitsgrenze (Risikoschwelle) ist bei der schon angesprochenen Rahmenzielsetzung festzulegen.

Im weiteren Sinne umfasst die Gefährdungsanalyse auch die Identifizierung sowie Initiierung von Maßnahmen zur Behebung festgestellter Verfahrensdefizite und damit die Reduzierung des Schadenspotenzials durch Rechtsnormverstöße. Dabei muss die Compliance-Funktion – wie jede Funktion in einer Bank – wirtschaftlich arbeiten. Diese Aufgabenstellung klingt fast wie eine „Quadratur des Kreises", der mit einem vierstufigen Verfahren begegnet werden kann (Abbildung 7).[16]

In der ersten Stufe werden die zu betrachtenden (Prozess-)Bereiche auf den Einhaltungsgrad relevanter Rechtsnormen untersucht. Die Bereiche WpHG-Compliance, Zentrale Stelle, Datenschutz und Verbraucherschutz sind hierbei obligatorisch einzubeziehen. Die BaFin sieht diese „unter Compliance-Gesichtspunkten" mit besonderen Risiken behaftet an.[17]

Bei der Evaluation der Bereiche haben sich folgende sechs Faktoren als zweckmäßig erwiesen: Mitarbeiterqualifikation, Mitarbeiterkapazität, IT-Workflow, Information, Prozessablauf und Vertragsmanagement. Sofern ein (relativ) hoher Einhaltungsgrad ermittelt wird, spricht vieles dafür, dass Compliance-Risiken wirksam verhindert werden. Es besteht kein weiterer Handlungsbedarf und eine – oftmals aufwandsintensive – quantitative Bewertung wird obsolet. Ein mittlerer beziehungsweise niedriger Einhaltungsgrad ist ein Indikator für die Notwendigkeit einer Verfahrensverbesserung. Oftmals lässt sich dieser durch geeignete Maßnahmen mit einem geringen Aufwand kurzfristig beheben. Diese Entwicklung ist Gegenstand des zweiten Schrittes. Hierfür sind Aufwandsgrenze und die maximal tolerierbare Umsetzungsfrist institutsspezifisch festzulegen.

Liegen die Kosten der Maßnahme über der Aufwandsgrenze (oder kann die gesetzte Frist nicht eingehalten werden), ist es aus wirtschaftlichen Gesichtspunkten sinnvoll, eine quantitative Risikobewertung nach Schadenshöhe und Eintrittswahrscheinlichkeit durchzuführen. Dieser dritte, arbeitsintensive Schritt wird also nur für eine kleine Teilmenge gefährdeter Prozess- beziehungsweise Rechtsnormbereiche durchgeführt.

Anwendung von Normstrategien

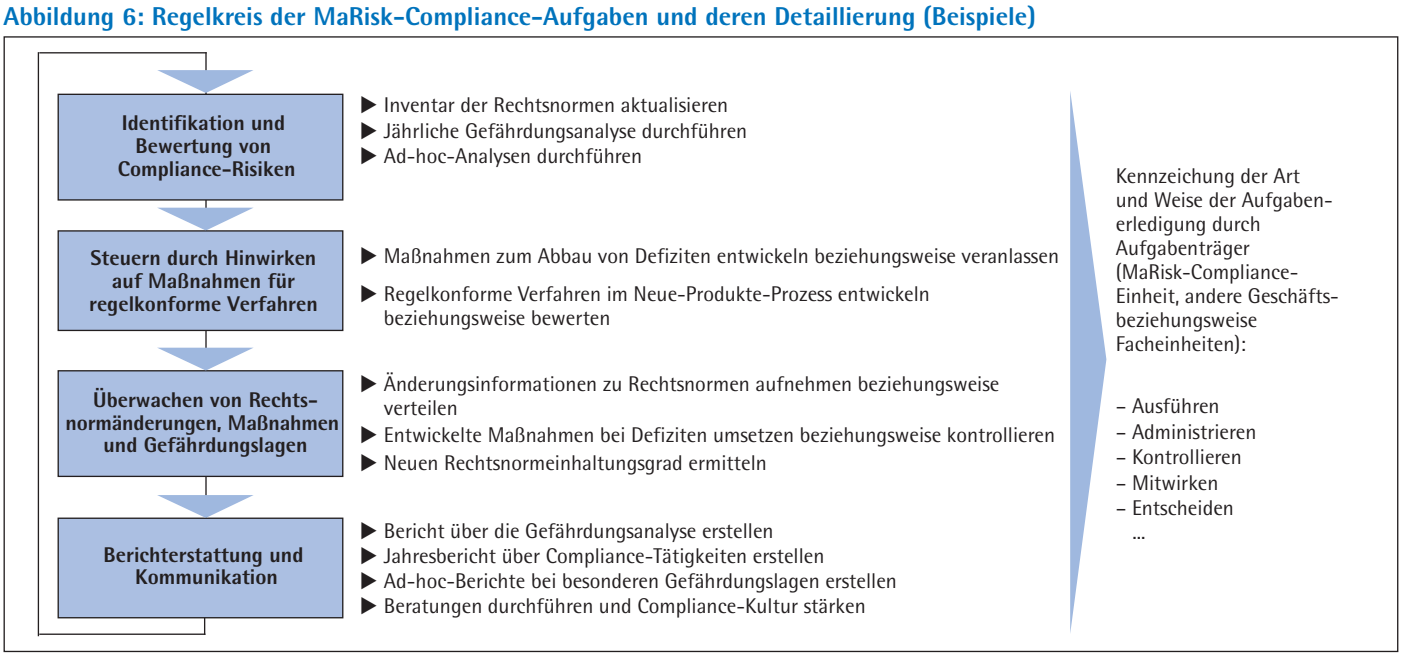
Diese Bereiche können anhand ihrer zweidimensionalen Bewertung eindeutig einer Risikoklasse in dem schon angesprochenen Risikodiagramm zugeordnet werden. Damit könnte die Anwendung von Normstrategien zum Tragen kommen: Risikoakzeptanz bei niedriger Risikoklasse (unterhalb der Risikoschwelle), Maßnahmeninitiierung bei hoher Klasse oder temporäre Akzeptanz beziehungsweise Risikominderung bei mittlerer Klasse. Die Anwendung solcher Normstrategien und die Entscheidungskompetenzen sind – wie die schon behandelte Risikoschwelle – Fragen der Gesamtbanksteuerung und letztendlich vom Vorstand zu entscheiden.

Optimierungsprozess nach Projektende nicht abgeschlossen

Die Optimierung von Compliance-Strukturen wird auch nach dem Abschluss eines Weiterentwicklungsprojektes auf der Tagesordnung in den Instituten bleiben. Bankenaufsicht, Kreditwirtschaft und Wissenschaft werden Profiteure und zugleich Treiber dieses Prozesses bleiben.

Die Bankenaufsicht wird durch die sich entwickelnden Best-Practice-Lösungen die Chance erhalten, die von ihnen aufgestellten Compliance-Anforderungen zu schärfen. Damit entfallen aufwändige Auslegungsdiskussionen von Bankenaufsicht und Kreditwirtschaft und möglicherweise auch die eine oder andere ineffiziente Compliance-Struktur in der Bankpraxis (Gürtel und Hosenträger).[18] Bei den aufsichtlichen Klarstellungen sollte die Aufsicht die begrüßenswerte Hinwendung zu einer stärker prinzipienorientierten Bankenregulierung unter Berücksichtigung von Art, Umfang und Risiko geschäftlicher Aktivitäten konsequent weiterverfolgen. Ansonsten bestünde die Gefahr, dass der

Abbildung 6: Regelkreis der MaRisk-Compliance-Aufgaben und deren Detaillierung (Beispiele)

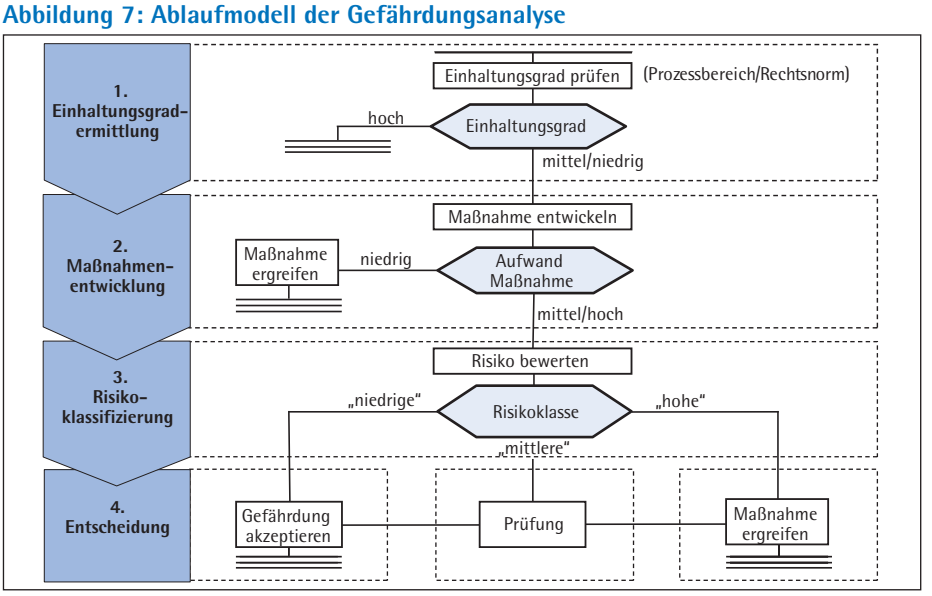


Spielraum kleinerer Banken mit immer größer werdenden Fixkosten unnötig eingeengt wird und sie für die Sündenfälle der Großen mit büßen müssen.[19] Gezahlte beziehungsweise erwartete „Spitzen"-Bußgelder von 70 Milliarden US-Dollar in Amerika (Bank of America) oder von 46 Milliarden US-Dollar beim Zweitplatzierten, in diesem Fall aus Europa (Lloyds BG), machen deutlich, wo der Compliance-Bedarf tendenziell besteht.[20]

Die Bankpraxis kann insofern auf den Optimierungszug aufspringen, als sie den überbetrieblichen und den innerbetrieblichen Informationsaustausch forciert. Beim zuerst genannten Austausch könnten beispielsweise die Bankenverbände die Best-Practice-Lösungen sammeln und den Instituten zur Verfügung stellen. Auf innerbetrieblicher Ebene können Effizienz- und Effektivitätsgewinne durch einen regelmäßigen Informationsaustausch von Compliance, Risikocontrolling und Revision erzielt werden (Säulen des Risikomanagements). Dort, wo die Revision Regelverstöße erkannt hat und sie deren Beseitigung überwacht, braucht die Compliance-Einheit keine Arbeitsschwerpunkte mehr legen. Die zunehmende Nutzung von Schadensfalldatenbanken und Risikoinventuren des Controllings operationaler Risiken wird eine gezielte und effektive Compliance-Arbeit unterstützen. Nicht zu unterschätzen ist auch die Zusammenarbeit der Compliance-Funktion mit der Rechtsabteilung und deren Erfahrungen mit den typischen Rechtsfällen in einem Institut.

Auch die Wissenschaft ist in dem Optimierungsprozess gefordert, hier in Form einer interdisziplinaren Zusammenarbeit von Jurisprudenz und Ökonomie. Ein Handlungsfeld ist beispielsweise die Entwicklung von Messgrößen für die MaRisk-Compliance-Effizienz beziehungsweise Effektivität. Letztendlich müssen sich die Fixkosten von Compliance-Strukturen lohnen. Hierbei könnte die Entwicklung der Ist-Vermögensschäden ein Ansatz sein; eine Reduktion oder das Beibehalten eines niedrigen Niveaus wäre als Erfolg zu buchen. Ein anderes, hiermit jedoch zusammenhängendes Feld aus dem Bereich der Organisationslehre wäre die Konzeption von Personalzumessungsmodellen mit Richtwerten für unterschiedliche Institutsarten und -größen.

Abbildung 7: Ablaufmodell der Gefährdungsanalyse



Fußnoten

1) Das englische Verb „to comply with something" bedeutet „etwas erfüllen, einhalten oder nachkommen".

2) Vgl. BaFin, Mindestanforderungen an das Risikomanagement (MaRisk), 14. Dezember 2012. Bei diesem Regelwerk handelt es sich um eine sogenannte Verwaltungsvorschrift zur Präzisierung der Anforderungen an eine ordnungsgemäße Geschäftsorganisation gemäß § 25a KWG. Die MaRisk-Compliance-Anforderungen sind in dem neuen Untermodul AT 4.4.2 MaRisk aufgeführt.

3) Der Begriff „Verfahren" umfasst in diesem Zusammenhang die organisatorisch-technische Vorgehensweise im Hinblick auf die Einhaltung von Rechtsnormen. Die Eigenschaft „wirksam" kann dann als vorhanden angesehen werden, wenn sowohl eine hinreichende Dokumentation des Verfahrens (nachvollziehbare schriftliche Fixierung) als auch eine entsprechende Handhabung in der Praxis vorliegen.

4) Das Modell der drei Verteidigungslinien beschreibt Rolle und Verantwortung des operativen Managements, des Risikocontrollings und der Compliance-Funktion bis hin zur Internen Revision im Hinblick auf ein effektives Risikomanagement. Vgl. hierzu: The Institute of Internal Auditors (IIA), IIA Position Paper: The Three Lines of Defense in effective Risk Management and Control, Januar 2013.

5) Vgl. BaFin-Schreiben an das Institut der Wirtschaftsprüfer vom 26. November 2013.

6) Gemäß dem neugefassten § 54a KWG können Geschäftsleiter von Banken bei Pflichtverstößen im Risikomanagement mit Freiheitsstrafen bis zu fünf Jahren oder Geldstrafen belegt werden. Es bestehen allerdings Bedenken hinsichtlich des strafrechtlichen Bestimmtheitsgebots und der Greifbarkeit der straftatbestandlichen Handlung. Vgl. Wegner, Carsten, Neue strafrechtliche Risiken, in: Betriebswirtschaftliche Blätter, 18. Oktober 2013, http://www.sparkassenzeitung.de (Stand: 14. September 2014).

7) Dieser Artikel gibt die persönliche Meinung der Autoren wieder, auch wenn Erkenntnisse aus einem Projekt zur Weiterentwicklung der MaRisk-Compliance-Funktion bei der Sparkasse Bremen eingeflossen sind.

8) Vgl. BaFin, Protokoll zur Sitzung des Fachgremiums MaRisk vom 24. April 2013 sowie EBA, Guidelines of Internal Governance, 27. September 2011.

9) IDW, PS 980 Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen, verabschiedet vom Hauptfachausschuss am 11. März 2011, http://www.idw.de (Stand: 9. September 2014).

10) Vgl. AT 4.4.2, Ziffer 1, Satz 2 MaRisk.

11) Vgl. Lindner, Bernd Michael, Schroeren, Dorit, Neueste Entwicklungen von Compliance in Banken durch die 4. MaRisk-Novelle, Seite 769, in: Zeitschrift für das gesamte Kreditwesen, Heft 15-2013, S. 766 bis 770.

12) Vgl. AT 4.4.2, Ziffer 2 MaRisk.

13) Vgl. hierzu beispielsweise Reichmann, Thomas, Diederichs, Marc, Risikobeurteilung, in: Horváth, Péter, Reichmann, Thomas (Hrsg.): Vahlens Großes Controllinglexikon, 2., neubearbeitete und erweiterte Auflage, München 2003, S. 669 f.

14) Vgl. AT 4.4.2, Ziffer 3 MaRisk.

15) Diese Verantwortungszuweisung entspricht der MaRisk-Anforderung (AT 4.4.2, Ziffer 1), dass „die Geschäftsbereiche für die Einhaltung rechtlicher Regelungen und Vorgaben uneingeschränkt verantwortlich bleiben."

16) Vgl. Martens, Tom, Compliance-Management in Banken im Hinblick auf die Anforderungen der vierten MaRisk-Novelle, Universität Greifswald (Diplomarbeit), 2014, S. 31 bis 45.

17) Vgl. BaFin, BaFin Journal, Mitteilungen der Bundesanstalt für Finanzdienstleistungsaufsicht, März 2013, S. 17.

18) Wie ist beispielsweise das Zugeständnis der Aufsicht zu interpretieren, bestimmte Rechtsgebiete aus dem Tätigkeitsbereich der Compliance-Funktion grundsätzlich auszuklammern (beispielsweise Arbeitsrecht) oder auf eigene Aktivitäten im Wesentlichen zu verzichten (beispielsweise Rechnungslegung)? – Vgl. BaFin, Protokoll zur Sitzung des Fachgremiums MaRisk vom 24. April 2013, S. 2.

19) Mittlerweile mehren sich auch die Stimmen aus der Politik für eine generell differenzierte Bankenaufsicht in Europa (Hinweis: EBA-Leitlinien zur Internal Governance waren Triebfeder für die deutschen Compliance-Anforderungen!); vgl. Kühl, Carsten (früherer Finanzminister des Landes Rheinland-Pfalz), Europas Aufsicht muss kleineren Banken Luft lassen, in: Börsenzeitung, Frankfurt am Main, 29. August 2014.

20) Vgl. N. N., Commerzbank droht hohe Strafe, in: Börsenzeitung, Frankfurt am Main, 9. Juli 2014.