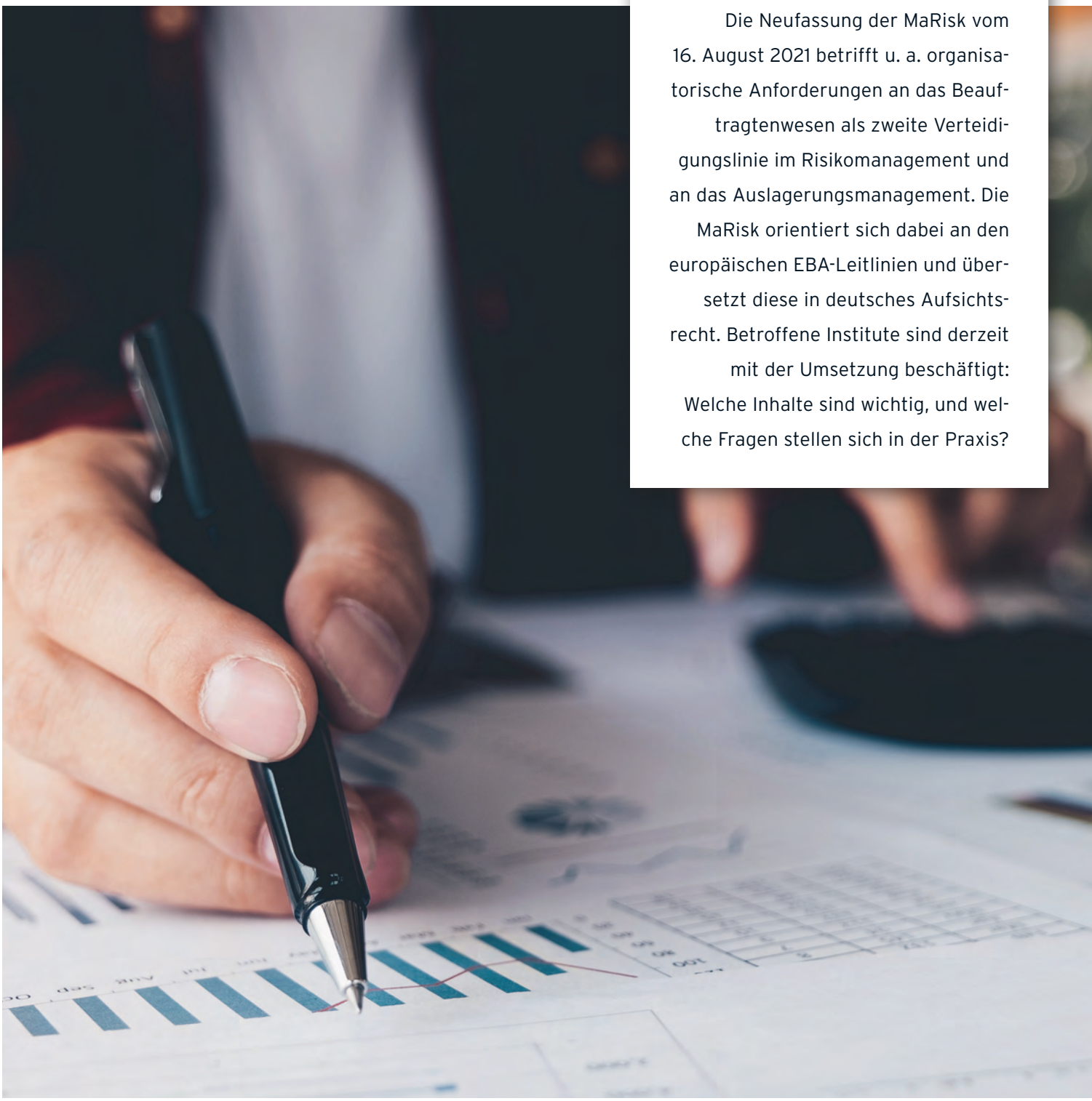
MARISK-NOVELLE 2021

Was die neuen Vorgaben für die Banken in der Praxis bedeuten



Die Neufassung der MaRisk vom 16. August 2021 betrifft u. a. organisatorische Anforderungen an das Beauftragtenwesen als zweite Verteidigungslinie im Risikomanagement und an das Auslagerungsmanagement. Die MaRisk orientiert sich dabei an den europäischen EBA-Leitlinien und übersetzt diese in deutsches Aufsichtsrecht. Betroffene Institute sind derzeit mit der Umsetzung beschäftigt: Welche Inhalte sind wichtig, und welche Fragen stellen sich in der Praxis?

Mit der Einführung der einheitlichen europäischen Bankaufsicht (Single Supervisory Mechanism, SSM) im Jahr 2014 entstand die Gefahr einer inhaltlichen Redundanz zwischen europäischen Normen und nationalen Anforderungen. Die frühere Erwartung einiger Beobachter, dass die deutsche MaRisk obsolet werden könnte, hat sich allerdings nicht bestätigt. Stattdessen wurden die Mindestanforderungen an das Risikomanagement seither vor allem zu einem Vehikel für die Umsetzung europäischer Richtlinien.

Hier gab es zwei Neufassungen im Oktober 2017 und im August 2021 mit erheblichen inhaltlichen Erweiterungen. Die aktuelle Neufassung enthält u. a. neue und geschärfte Vorgaben zum Beauftragtenwesen und zum Auslagerungsmanagement, die sich an den korrespondierenden EBA-Leitlinien für das Management von IKT- und Sicherheitsrisiken und zu Auslagerungen orientieren (IKT steht für Informations- und Kommuikationstechnologie.)

Bei der Umsetzung von EBA-Leitlinien verfügen die nationalen Aufsichtsbehörden grundsätzlich über einen Ermessensspielraum, sodass es zu inhaltlichen Unterschieden zwischen EBA-Leitlinien und nationalen Vorschriften kommen kann. Die neue MaRisk gilt ab sofort mit einer Übergangsfrist bis Ende des Jahres 2021. Eine angemessene Umsetzung vor dem Hintergrund individueller Gegebenheiten ist für die Institute ökonomisch bedeutend, weil die neuen Regelungen Auswirkungen auf regulatorisch bedingte Sockelkosten für notwendige Mitarbeiterkapazitäten haben und die Fähigkeit beeinflussen, Kostenreduktionen durch Inanspruchnahme spezialisierter Dienstleister zu realisieren.

Geltungsbereich und Proportionalität

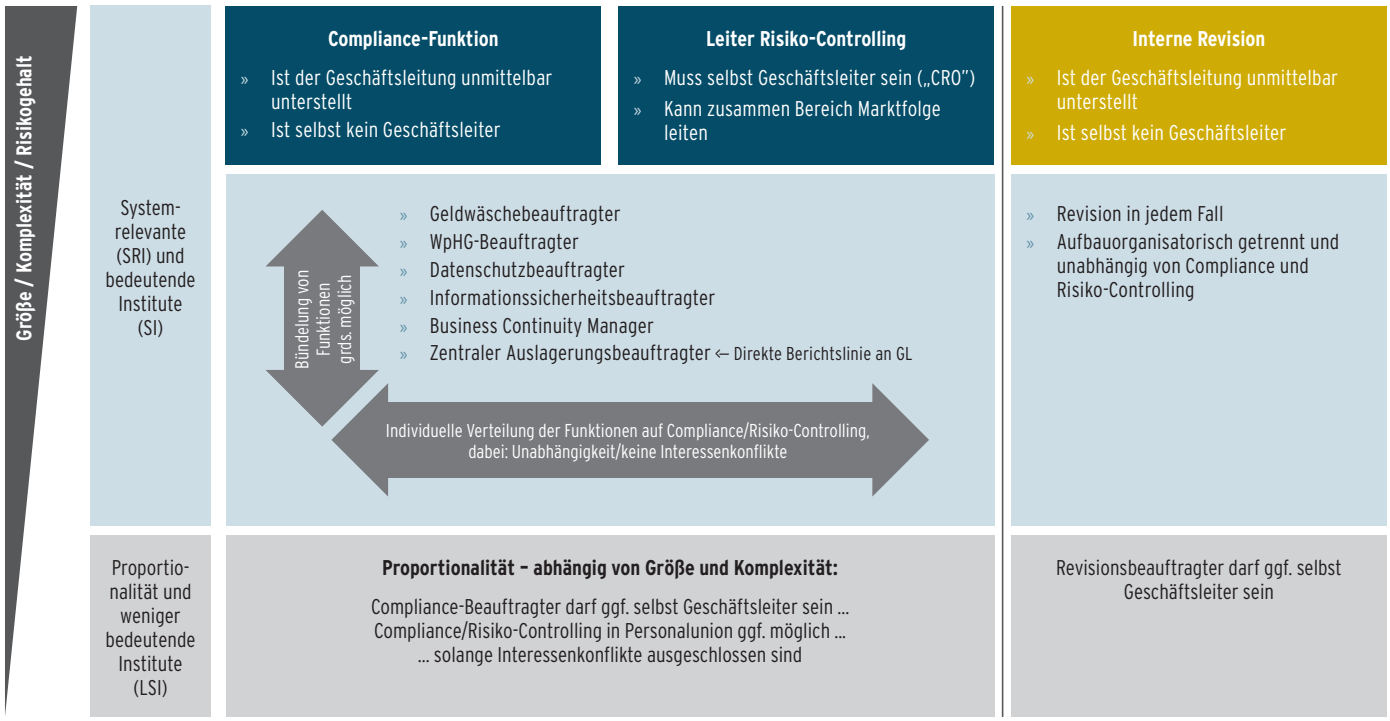
Die neue MaRisk verschärft Anforderungen an besondere Funktionen im Risikomanagement generell dadurch, dass diese nun nicht mehr nur für die systemrelevanten Institute gelten, sondern bereits für bedeutende Institute. Institute gelten als bedeutend, wenn sie die Kriterien von Artikel 6 der SSM-Verordnung erfüllen und deshalb direkt von der EZB beaufsichtigt werden. Dabei handelt es sich in Deutschland (Stand Juli 2021) um 21 Konzerne und ihre (teilweise internationalen) Tochter-Institute. Für die Klassifizierung ist vor allem das Größenkriterium ausschlaggebend, hier liegt die Schwelle bei einer Bilanzsumme von über 30 Mrd. €. Deshalb bleiben im Wesentlichen alle Sparkassen und Genossenschaftsbanken außerhalb des Geltungsbereichs. Ausnahmen betreffen die Hamburger Sparkasse und die Sparkasse Mittelholstein (als Töchter der Haspa Finanzholding), die Frankfurter Sparkasse (als Tochter der Helaba) sowie die Deutsche Apotheker- und Ärztebank (aufgrund ihrer eigenen Größe). Der Hinweis, dass kleine Tochterinstitute wie die Sparkasse Mittelholstein von den verschärften Anforderungen ausgenommen werden sollten, wurde im Konsultationsprozess von der BaFin nicht aufgegriffen.

Anforderungen der neuen MaRisk, die das Auslagerungsmanagement betreffen, sind teilweise auch für weniger bedeutende Institute relevant. So müssen sie künftig in jedem Fall einen zentralen Auslagerungsbeauftragen benennen (AT 9 Tz. 12), der direkt an die Geschäftsleitung berichtet oder selbst Mitglied der Geschäftsleitung ist, und ein zentrales Auslagerungsregister einrichten (AT 9 Tz. 14). Die generelle Notwendigkeit eines Auslagerungsbeauftragten geht über die Vorgaben der EBA-Leitlinie hinaus.

Compliance-Funktion und Risiko-Controlling

Schon bisher muss jedes Institut eine Compliance-Funktion einrichten (AT 4.4.2 Tz. 1), um den Risiken aus der Nichteinhaltung aufsichtsrechtlicher Regelungen vorzubeugen und entgegenzuwirken. Bei bedeutenden Instituten muss die Compliance-Funktion fortan grundsätzlich aufbauorganisatorisch eigenständig (AT 4.4.2 Tz. 4) sein. In ihr dürfen ausdrücklich weitere Compliance-nahe Auf-

1 | Übersicht: Beauftragtenwesen nach MaRisk



Quelle: Berg Lund & Company.

gaben wahrgenommen werden (z. B. WpHG-Compliance, Geldwäschebeauftragter, Informationssicherheitsbeauftragter, Datenschutz).

In der Konsultation der MaRisk Ende 2020 wurde zunächst vorgesehen, einige Funktionen wie Auslagerungen, Informationssicherheit und Business Continuity Management dem Risiko-Controlling zuzuordnen und nicht der Compliance-Einheit. Diese Trennungspflicht wurde zum Glück nicht in die finale Version übernommen; sie hätte eine unnötig kleinteilige und fragmentierte Besetzung der Überwachungsfunktionen erfordert.

Viele Institute haben ihr Auslagerungsmanagement in den letzten Jahren als Compliance-nahe Aufgabe entwickelt, sodass ihnen erheblicher Transformationsbedarf entstanden wäre. Eine Trennungspflicht wäre zudem sowohl über die Anforderungen der EBA-Leitlinie als auch über bisherige Anforderungen an systemrelevante Institute hinausgegangen und hätte auch nicht zu Tz. 4.6 BAIT gepasst, wonach Institute „die Funktion des Informationssicherheitsbeauftragten grundsätzlich mit anderen Funktionen im Institut kombinieren" können.

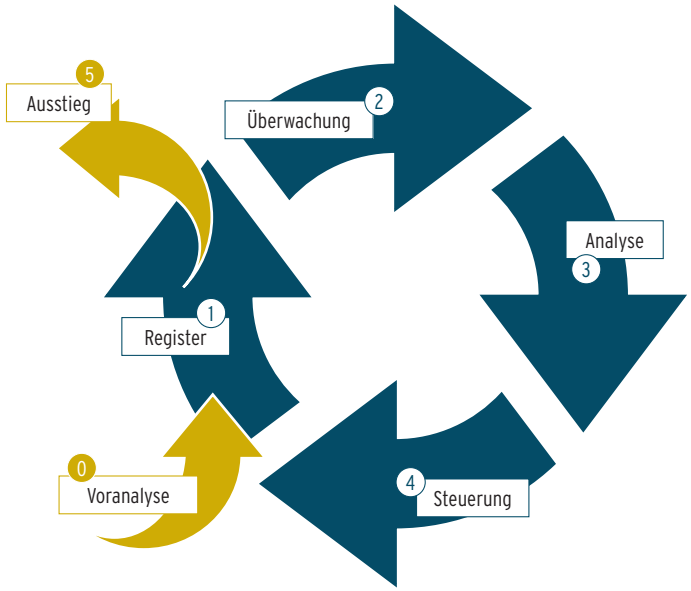
Ziel- oder Interessenkonflikte durch Bündelung mehrerer Kontrollfunktionen in der Compliance-Funktion sind nicht generell erkennbar, müssen aber im Einzelfall und unter Berücksichtigung individueller Besonderheiten untersucht werden. Die Analysen und Kontrollen, die hinsichtlich Informationssicherheit, Business Continuity und Auslagerungen notwendig sind, passen normalerweise inhaltlich gut zum Auftrag der Compliance-Funktion. Aus dem Verlauf der Konsultation ist ersichtlich, dass die Aufsicht im Fall solcher Zusammenfassungen ein besonderes Augenmerk auf die nötige Unabhängigkeit der ausführenden Personen legen wird.

Durch den Wegfall der Trennungspflicht in der finalen Version der MaRisk haben Institute weiterhin die Möglichkeit, Synergien zu realisieren und den Abstimmungsaufwand zwischen Überwachungsfunktionen zu reduzieren, wodurch die Effektivität des Risikomanagements insgesamt gesteigert werden kann. Beispielsweise können die Funktionen zu Informationssicherheit und Business Continuity in Personalunion wahrgenommen werden, was bei vielen Instituten gut funktioniert.

Die Leitung der Risikocontrolling-Funktion hat grundsätzlich durch einen Geschäftsleiter zu erfolgen (AT 4.4.1 Tz. 5). Dieser darf zwar gleichzeitig den Bereich Marktfolge verantworten, aber weder den Bereich Finanzen/Rechnungswesen noch den Bereich Organisation/IT. Im Gegenzug zur Ausweitung der Geltung dieser Regelung auf bedeutende Institute sieht die neue MaRisk nun eine Öffnungsklausel unter Berufung auf das Proportionalitätsprinzip vor. Demnach ist die Wahrnehmung der Risiko-Controlling-Funktion gegebenenfalls in Personalunion mit der Leitung der Compliance-Funktion oder einer anderen leitenden Person möglich, sofern eine separate Besetzung unverhältnismäßig wäre und hieraus kein Interessenkonflikt entsteht.

Zur Überwachung und Steuerung von Auslagerungen muss jedes Institut einen zentralen Auslagerungsbeauftragten ernennen (AT 9 Tz. 12), der über eine direkte Berichtslinie zur Geschäftsleitung verfügt. ▸ 1

2 | Auslagerungszyklus nach MaRisk im Überblick



0 Voranalyse	Due-Diligence-Prüfung Risikobewertung Identifikation möglicher Interessenkonflikte
1 Register	Vertragsverhandlung und -abschluss Erfassung im Auslagerungsregister Erhebung Mindestinformationen
2 Überwachung	Kontinuierliche Überwachung KPI/KRI Einhaltung Vereinbarungen/Anforderungen Nutzung Zugangs-, Informations- und Prüfungsrechte
3 Analyse	Regelmäßige Risikobewertung Weiterverlagerungen, Konzentrationsrisiken Auswertung qualitativer Informationen
4 Steuerung	Kommunikation mit Dienstleister Ergreifen von Abhilfemaßnahmen Aktualisierung vertraglicher Bedingungen
5 Ausstieg	Dokumentierte Ausstiegspläne Rückverlagerung oder Übertragung an Dritte Gewährleistung störungsfreie Leistungserbringung

Quelle: Berg Lund & Company.

Auslagerungen, sonstiger Fremdbezug und Weiterverlagerungen

Zwar wurden die Anforderungen an das Auslagerungsmanagement in AT 9 der MaRisk recht umfangreich angepasst. Die grundlegende Definition von Auslagerungen stellt aber unverändert darauf ab, ob in Anspruch genommene Leistungen ansonsten vom Institut selbst erbracht würden. Ist dies nicht der Fall, handelt es sich regelmäßig um sonstigen Fremdbezug von Leistungen. Zur Illustration des Unterschieds dienen mehrere Fallbeispiele in AT 9 Tz. 1 (Erläuterungen), die nun zusätzlich Ratingagenturen, globale Zahlungsverkehrsdienstleister sowie Rechtsgutachter umfassen.

Zwar bedeuten aufsichtsrechtliche Definitionen anhand von exemplarischen Beispielen oft Auslegungsunsicherheiten. Im vorliegenden Fall begrüßen viele Institute jedoch die resultierende Flexibilität der Regelung.

Neu ist die Anforderung, dass jedes Institut ein Auslagerungsregister einzurichten hat (AT 9 Tz. 14), das alle Auslagerungen sowie wesentliche Weiterverlagerungen erfasst. Diese Anforderung wurde mit der Verabschiedung des Finanzmarktintegritätsstärkungsgesetzes, das der Bundestag am 20. Mai 2021 verabschiedet hat, zusätzlich auch direkt in § 25b KWG verankert. Zu inhaltlichen Mindestanforderungen des Auslagerungsregisters verweist die MaRisk direkt auf die EBA-Leitlinie zu Auslagerungen 2.

Die Wesentlichkeit eines Auslagerungssachverhalts unter Risikogesichtspunkten wird ebenfalls durch zusätzliche Fallbeispiele geschärft (AT 9 Tz. 2, Erläuterungen). Diese Beispiele betreffen politische Risiken, mögliche Interessenkonflikte und Schutzbedarfe sowie Risikokonzentrationen, wenn mehrere Auslagerungssachverhalte mit demselben Auslagerungsunternehmen bestehen. Risikoanalysen sind dabei durch Szenarioanalysen (ebenfalls AT 9 Tz. 2, Erläuterungen) zu ergänzen, soweit dies sinnvoll und verhältnismäßig ist. Insgesamt erhöhen die Fallbeispiele und die Szenarioanalysen Aufwand und Komplexität für nötige Risikoanalysen. Die neue Anforderung, dass Weiterverlagerungen gemäß AT 9 Tz. 11 (Erläuterungen) ebenfalls nach Risikogesichtspunkten auf ihre Wesentlichkeit untersucht werden müssen, trägt hierzu ebenfalls bei. Eine Bewertung politischer Risiken ist für Institute inhaltlich herausfordernd und, besonders wenn sie das eigene Land betreffen, heikel.

Vertragsgestaltung und laufende Überwachung

Die neue MaRisk sieht vor, dass Institute Auslagerungsunternehmen verpflichten sollten (AT 9 Tz. 7), bei Vertragsende eine Übertragung der Leistungen zurück an den Auftraggeber oder an benannte Dritte unterstützen zu müssen. Informations- und Prüfungsrechte sollten möglichst auch für nicht-wesentliche Auslagerungen vereinbart werden. Die Formulierungen im Konjunktiv („sollten“) ist dabei von großer Bedeutung, weil ansonsten die Gefahr bestünde, dass Institute ihre Auslagerungsverträge großflächig im Rahmen der Übergangsfrist bis Ende 2021 nachverhandeln müssten. Stattdessen gehen Institute derzeit davon aus, dass es ausreicht, die zusätzlichen

Inhalte bei neuen Verträgen oder ohnehin anstehenden Nachverhandlungen einzubringen.

Anstelle einer regelmäßigen Beurteilung wesentlicher Auslagerungen verlangt die neue MaRisk (AT 9 Tz. 9) eine „laufende" Überwachung anhand von Key Performance/Risk Indicators auf Basis vertraglich vereinbarter Informationen des Auslagerungsunternehmens. Es ist unklar, ob die BaFin hiermit tatsächlich ständige Überwachungsaktivitäten bei jeder wesentlichen Auslagerung einfordern will und wie die Überwachung zu erfolgen hat, um als laufend zu gelten.

Befugnis eines Auslagerungsunternehmens und „Empty Shell"-Regel

Ein auslagerndes Institut muss nach AT 9 Tz. 4 (Erläuterung) sicherstellen, dass ein Auslagerungsunternehmen außerhalb des Europäischen Wirtschaftsraums (EWR) nach dem Recht seines Sitzlands zur Erbringung der Leistungen befugt ist und von den dortigen Aufsichtsbehörden überwacht wird, wenn dies nach EU-Regeln erforderlich wäre. Diese Anforderung erschwert internationale Auslagerungen erheblich, weil sie Gutachten zur hiesigen und dortigen rechtlichen Situation erforderlich machen kann.

Zudem müssen Auslagerungen bei Veränderungen der Rechtslage neu bewertet werden, sodass eine regelmäßige Überprüfung notwendig wird. Unklar bleibt, ob Auslagerungen an ausländische Auftragnehmer, die nach dortiger Rechtslage nicht aufsichtspflichtig sind, überhaupt noch in Anspruch genommen werden können, wenn sie es nach EU-Recht wären.

Der aufsichtsrechtliche Rahmen für Banken ist mittlerweile derart eng und kostspielig geworden, dass es vielen Konzernen ökonomisch sinnvoll erscheint, ausschließlich solche Geschäftstätigkeiten innerhalb einer Vollbank zu betreiben, die eine solche Lizenz zwingend erfordern. Bei US-amerikanischen Großbanken sind aus diesem Grund sukzessive gesellschaftsrechtliche Restrukturierungen seit Jahren zu beobachten. Auch ohne Restrukturierungen können Auslagerungen diesen Trend unterstützen. AT 9 Tz. 4 MaRisk verbietet nun ausdrücklich Auslagerungen, die dazu führen, dass ein Institut „nur noch als leere Hülle (empty shell) existiert". Die Formulierung in dieser Klarheit ist ein bemerkenswertes Eingeständnis der BaFin bzw. der EBA zu Nebenwirkungen der intensiven Regulierung.

Institutsverbünde und Notfallmanagement

Für „weniger bedeutende" Institute ist die Zentralisierungsmöglichkeit in Institutsgrup-

FAZIT

Die MaRisk-Novelle schärft organisatorische Pflichten im Risikomanagement bedeutender Institute. Dabei erhält sie wichtigen individuellen Gestaltungsspielraum, den jedes betroffene Institut unverzüglich nutzen muss. Die umfangreiche Überarbeitung und Erweiterung der Anforderungen an das Auslagerungsmanagement verursachen auch bei „weniger bedeutenden" Instituten Handlungsbedarf. Neben der Ernennung eines zentralen Auslagerungsbeauftragten und der Einrichtung eines Auslagerungsregisters sind viele detaillierte Regelungen umzusetzen.

pen und Verbünden (AT 9 Tz. 15) von großer Bedeutung. Diese Erleichterung ist besonders in Deutschland wichtig: Sie stellt den aufsichtsrechtlichen Rahmen für das Auslagerungsmanagement insbesondere innerhalb der Sparkassen-Finanzgruppe und innerhalb der genossenschaftlichen Finanzgruppe klar.

Die Regeln zur Zentralisierung des Auslagerungsmanagements enthalten einen Verweis auf das Notfallmanagement nach AT 7.3 Tz. 2. Demnach müssen im Fall der Auslagerung von zeitkritischen Aktivitäten und Prozessen die Notfallkonzepte von Auftraggeber und Auftragnehmer aufeinander abgestimmt sein. Diese Anforderung ist insofern weitgehend, als ein Auftragnehmer, der für viele Institute gleichzeitig Leistungen erbringt – was in Institutsverbünden der Regelfall ist –, diese nicht individuell auf jeden Auftraggeber abstimmen kann. Im Umkehrschluss bedeutet dies, dass Sparkassen und Genossenschaftsbanken sich auf die Notfallkonzepte ihrer zentralen Verbunddienstleister einstellen müssen.

Die Einrichtung des zentralen Auslagerungsregisters darf grundsätzlich auf Gruppen- oder Verbundebene erfolgen, solange der Zugriff auf das individuelle Register eines Instituts bei Bedarf ohne größere Verzögerung möglich ist.

Die Compliance-Funktion, die Risiko-Controlling-Funktion und die Interne Revision dürfen innerhalb einer Institutsgruppe vollständig ausgelagert werden (AT 9 Tz. 5), sofern das auslagernde Institut für die Gruppe als solche nicht wesentlich ist. ▸ **2**

Autor

Dr. Tobias Sander ist Senior Manager bei Berg Lund & Company.