FRANKFURTER ARBEITSKREIS
COMPLIANCE & GOVERNANCE

Frankfurter Arbeitskreis Compliance & Governance
Expertenzirkel MaRisk-Compliance
E-Mail: mco@frankfurter-arbeitskreis.de

Stellungnahme

zur Konsultation 14/2020 Mindestanforderungen an das Risikomanagement der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) 04.12.2020

Frankfurt, 04.12.2020

FRANKFURTER ARBEITSKREIS
COMPLIANCE & GOVERNANCE

Hintergrund / Wer wir sind:

Der Frankfurter Arbeitskreis Compliance & Governance ist ein Forum für den fachlichen Austausch über Anforderungen, Erfahrungen und Best-Practice von Compliance- und Governance-Themen. Mit über 200 Mitgliedern repräsentiert der Arbeitskreis mehr als 100 große und mittelgroße Banken aus allen drei Säulen des Bankgewerbes. Ziele sind über den vorgenannten, fachlichen Austausch hinaus die Erarbeitung struktureller, konzeptioneller oder technischer Mehrwerte in den Expertenzirkeln für die Governance Risk- und Compliance-Community, die in praktikable Standards, Veröffentlichungen, Hilfestellungen, Checklisten, Tools, Seminare, etc. einfließen. Bei unserer Arbeit stehen immer die praktikablen Lösungen, nicht verbandspolitische Interessen, im Vordergrund.

Stellvertretend für den Expertenzirkel MaRisk Compliance geben wir: Karsten Büll, Judith Schwinger, Tabea Jarocki und Martin Daumann die vorliegende Stellungnahme zur Konsultation MaRisk-Novelle ab.

Allgemeines

Am 26.10.2020 hat die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) gemeinsam mit der Deutschen Bundesbank eine Konsultation zur Neufassung des Rundschreibens 09/2017 (BA) - Mindestanforderungen an das Risikomanagement – MaRisk gestartet. Die Überarbeitung ist zuvorderst auf Änderungen der internationalen Regelsetzung zurückzuführen.

Der Frankfurter Arbeitskreis Compliance & Governance begrüßt (grundsätzlich) die kontinuierliche Aktualisierung und Überarbeitung des Rundschreibens für die angemessene und wirksame Ausgestaltung des Risikomanagements der Institute. In unserer Stellungnahme haben wir uns auf einzelne, aus der Mitte unseres Expertenzirkels MaRisk intensiv diskutierte, Aspekte der vorliegenden MaRisk-Novelle konzentriert.

Basierend auf den Erfahrungen zu Umsetzungen regulatorischer Anforderungen in den Instituten regen wir eine Umsetzungsfrist für die Implementierung der modifizierten Anforderungen an. Insbesondere für Institute, die zu den weniger bedeutenden Instituten zählen und auch nicht einer direkten Aufsicht durch EZB unterliegen, bedeuten die neuen Anforderungen erhebliche Umsetzungsaufwände. Insoweit ist gerade für die kleineren Institute die Anmerkungen auf der BaFin-Internetseite zur Veröffentlichung der MaRisk-Novelle (https://bit.ly/3lH5FbY) nicht vollumfänglich nachvollziehbar. Zudem sehen sich alle Institute auch mit den Herausforderungen der Covid 19-Pandemie konfrontiert. In Abhängigkeit des Veröffentlichungszeitpunktes der novellierten MaRisk halten wir eine Frist bis zum 31.12.2021 für angemessen.

FRANKFURTER ARBEITSKREIS
COMPLIANCE & GOVERNANCE

Zu AT 4.4.2 TZ 4 Eigenständigkeit der Compliance

4	~~Systemrelevante~~ ~~Große und komplexe~~ Institute haben für die Compliance-Funktion eine eigenständige Organisationseinheit einzurichten.	**Eigenständige Compliance-Einheit** In der eigenständigen Einheit für die Compliance-Funktion dürfen auch weitere, Compliance-nahe Bereiche angesiedelt sein (z. B. WpHG-Compliance, Geldwäschebeauftragter, Datenschutz). Andere Bereiche (z. B. Auslagerungsbeauftragter und -management, Informationssicherheitsbeauftragter und -management, Business Continuity Management), insbesondere Bereiche, die dem Risikocontrolling zuzuordnen sind, dürfen nicht in der Compliance-Einheit angesiedelt werden.

Die Compliance-Funktion wurde mit Novellierung der MaRisk 2012 als Bestandteil der Besonderen Funktionen nach AT 4.4. MaRisk verbindlich eingeführt und war mit Frist zum 01.01.2014 in den Instituten zu implementieren. Im Rahmen der vergangenen Novellen wurden hier lediglich marginale Anpassungen vorgenommen, um die Etablierung von Marktstandards zu ermöglichen. Wir sehen in der aktuellen Konsultation Konkretisierungsmaßnahmen und erwarten auch in künftigeren Novellierungen weitere Ausgestaltungen. Wir würden in diesem Kontext auf Basis der der EBA-Leitlinien für die Kreditvergabe und Überwachung (EBA/GL/2020/06) Konkretisierungen zu Überwachungshandlungen begrüßen. Eine solche Konkretisierung fördert eine angemessene und wirksame Umsetzung in den Instituten, dies hat die Entwicklung der Mindestanforderungen an die Compliance-Funktion und weitere Verhaltens-, Organisations- und Transparenzpflichten – MaComp und deren Umsetzung in den Instituten gezeigt.

In den letzten Jahren wurden durch die MaRisk und die BAIT weitere Funktionen geschaffen, welche wir in der 2nd line of defence gemäß den EBA-Guidelines zur internen Governance (EBA/GL/2017/11) sehen. Hier seien vor allem die relativ neuen Funktionen „Informationssicherheitsbeauftragter“ und „Auslagerungsbeauftragter“ genannt. Wir begrüßen die konkrete Ausgestaltung der Anforderungen an diese Funktionen, da sie im Gesamtkontext Compliance unterstützend dazu beitragen, die Angemessenheit, Wirksamkeit und die Sicherheit in den Themenkomplexen „Informationssicherheit“ und „Auslagerungen“ zu erhöhen. Aus unserer Sicht handelt es sich um themenspezifische „Compliance-Funktionen“ in der zweiten 2nd line of defence. Dies bedeutet, dass diese der 1st line of defence Vorgaben und Systeme vorgeben und deren Einhaltung überwachen, Defizite managen und reporten; insoweit lassen sich diese Tätigkeiten den klassischen Compliance-Tätigkeiten zuordnen.

Anhand der aufsichtsrechtlichen Texte zu den vorgenannten Funktionen sowie deren Vergleich mit regulatorischen Anforderungen bereits länger bestehender Compliance-Funktionen lässt sich diese vorgenannte Auffassung untermauern. Die Anforderungen an das Berichtswesen, die Unterstützung und Beratung der Geschäftsleitung hinsichtlich der Einhaltung der rechtlichen Regelungen und Vorgaben im jeweilig relevanten Themenkomplex, Anforderungen an die Qualifikation von Mitarbeiterinnen/Mitarbeitern in den Compliance-Funktionen und nicht zuletzt die Regelungen zu Implementierungs- bzw. Überwachungsaufgaben zeigen auf, dass die verschiedenen Funktionen zu den Compliance-Funktionen, der 2nd line of defence zugehörig, zuzuordnen sind. Zum anderen zeigt der Vergleich auf, dass die aufsichtsrechtlich beschriebenen Tätigkeiten vergleichbare, wenn nicht auch identische Zielrichtungen verfolgen.

Inhaltlich nimmt die Komplexität des Risikomanagements und der Gesamtbanksteuerung stetig zu. Dabei spielen die nicht-finanziellen Risiken tendenziell eine wachsende Rolle, so z.B. Nachhaltigkeitsrisiken. Viele Banken haben dies erkannt und haben oder sind gerade dabei, sämtliche Funktionen mit dieser Aufgabe zu bündeln. Hintergrund ist es ein einheitliches Sys-

tem zum Erkennen, Steuern und Berichten, der so genannten Non-Financial-Risk (NFR) aufzubauen. Eine Zusammenfassung der Funktionen fördert unserer Auffassung nach den Austausch dieser Funktionen und führt zu einer Angleichung der Methoden. Das entspricht auch dem sich weiter entwickelten Verständnis der nicht-finanziellen Risiken. Zahlreiche Banken haben hier in der jüngsten Vergangenheit begonnen, dies aufzubauen. Waren noch vor einigen Jahren Geldwäschebeauftragte, Informationssicherheitsbeauftragte und Compliance-Beauftragte sowie die zentralen Stellen, sonstige strafbare Handlungen, IKS und BCM verschiedenen Organisationseinheiten angesiedelt, so haben viele Institute erkannt, dass eine konsolidierte Betrachtung dieser Risiken nicht nur effizient ist, sondern für das Risikomanagement einen neuen Qualitätsstandard schaffen kann.

Eine Zusammenfassung der Funktionen beugt den erkannten und vorhandenen Risiken in einer heterogenen Organisationsstruktur des NFR-Managements vor. Durch eine hohe Anzahl von Schnittstellen entstehen Redundanzen oder Lücken in Prozessen sowie im Überwachungs- und Kontrollsystem der 2nd line of defence. Inhaltliche Überschneidungen verschiedener Analysen (bspw. MaRisk-Risikoanalyse, OpRisk-Assessment, Gefährdungsanalyse Geldwäsche- und Betrugsprävention) führen zu inhomogenen Einschätzungen operationeller Risiken. Insgesamt führt dies zu einer ineffizienten Ressourcenbelastung. Eine Harmonisierung der Instrumente und daraus resultierenden Aggregierung im Berichtswesen für die relevanten Entscheider im Hause verhindern das Risiko einer Überschneidung von Informationen oder sogar divergierenden Ergebnissen. Es ist somit nur konsequent, diesen Schwächen eines heterogenen Non-Financial-Risk-Managements durch einen konsolidierten Ansatz zu begegnen.

Das angestrebte Ansiedlungsverbot würde bei diesen Instituten zu teils hohen Reorganisationskosten führen. Es gibt keinen erkennbaren Grund, verschiedene Funktionen der 2nd line of defence nicht zu koppeln. Dadurch werden wie vorstehend dargestellt im Gegenteil Synergiepotenziale genutzt.

Insbesondere NFR wächst in vielen Instituten mit Compliance zusammen bzw. wird den Compliance-Funktionen zugewiesen. Dagegen werden die „klassischen“ finanziellen Risiken im Risikocontrolling verortet. So ist auch die Betonung der Zusammenarbeit zwischen diesen Funktionen laut Tz. 193 der EBA-Leitlinien zur internen Governance zu interpretieren. Daher können wir das geplante Ansiedlungsverbot der im Entwurf genannten Funktionen nicht nachvollziehen.

Eine hiervon differenziert zu betrachtende Funktion ist der Datenschutzbeauftragte eines Instituts, hierzu sei auf unsere Ausführungen am Ende dieses Abschnittes zu AT 4.4.2 TZ 4 verwiesen.

Die Finanzinstitute befinden sich aktuell in einer Phase der digitalen Transformation, die eine hohe Geschwindigkeit durch immer kürzere Innovationszyklen und einen umfassenden Wandel von ihnen fordert. Dies zeigt sich in veränderten IT-Infrastrukturen und immer mehr Auslagerungen von IT-Services. Der Trend geht hin zu einer intelligenten Vernetzung innovativer Kommunikationsstrukturen. Durch den Einsatz künstlicher Intelligenz werden Prozesse und Verfahren für Mitarbeiter und Kunden effizienter gestaltet, um sich auf das Wesentliche konzentrieren zu können.

Es sollte auch nicht die derzeitige ökonomische und pandemische Lage außer Acht gelassen werden. Institute müssen in Zeiten niedriger bzw. negativer Zinsen und durch die aktuelle Covid19-Pandemie sehr unsicherer konjunktureller Aussichten auch noch rentabel wirtschaften. Dafür ist es insbesondere erforderlich, die eigene Wertschöpfungskette optimieren zu können, ohne von weitgehenden regulatorischen Vorgaben ausgebremst zu werden.

Wir begrüßen ausdrücklich die Benennung und Ausweitung von Beauftragten-Funktionen. Hierdurch werden klare Zuständigkeiten und Verantwortlichkeiten geschaffen. Jedoch gehört es zu der heutigen Arbeitswirklichkeit, dass Arbeitnehmer mehr als eine Aufgabe wahrnehmen und dabei auch teilweise in Konkurrenz stehende Ziele fördern / verfolgen im Sinne eines „sowohl als auch“. Daher ist es nur schwer nachvollziehbar, wenn hier konkrete Vorgaben / Verbote zu Ansiedlung innerhalb der 2nd line of defence gemacht werden. Es handelt sich sicherlich um eine herausfordernde Aufgabe, diese Tätigkeiten zu vereinbaren. Diese überschreitet jedoch unseres Erachtens keine „Gefahrenschwelle“, die eine verpflichtende Zuordnung außerhalb der institutsindividuellen Ausgestaltung der Organisation erfordern, zumal demgegenüber diverse (nachfolgend aufgezählte Synergiepotenziale) apodiktisch und ohne Öffnungsklausel abgeschnitten werden. Beispielhaft seien genannt:

- Die Nutzung der Compliance-Instrumente (z. B. Self-Assessments, Szenarioanalysen, Risikoindikatoren, Risikobewertung, Risikoanalysen) werden durch die OpRisk-Funktion erheblich unterstützt, da die OpRisk-Funktion zum einen die gleichen Instrumente nutzt und die Informationen aus den Ergebnissen der OpRisk-Instrumente die Compliance-Themen erheblich unterstützen.
- Gerade das Thema OpRisk unterstützt die Aufgabe von Controlling, die Transparenz über Compliance-Verstöße zu haben.
- Gerade die Synergien zwischen OpRisk und dem Compliance-Thema „sonstige strafbare Handlungen“.

Die genannten Beispiele verdeutlichen die Hebung von Synergiepotenzialen.

Eine Zusammenfassung der Funktionen beugt den erkannten und vorhandenen Risiken in einer heterogenen Organisationsstruktur des NFR -Management vor.

Die explizit genannten Funktionen Auslagerungsbeauftragter und -management, Informationssicherheitsbeauftragter und -management, Business Continuity Management werden als nicht Compliance-nahe Bereiche eingestuft. Diese Einstufung erschließt sich dem Arbeitskreis nicht, da es sich bei Funktionen wie bei der Compliance-Funktion um Funktionen der 2nd line of defence handelt, die jeweils mit der Begrenzung und Überwachung von Non Financial Risk und dem Hinwirken auf die Einhaltung gesetzlicher und aufsichtsrechtlicher Regelungen gleichgerichtete Ziele verfolgen.

Sollte die o. g. Regelung so zu interpretieren sein, dass die o. g. Funktionen nicht in einem Bereich zusammengefasst werden dürfen, würde dies in als groß und komplex einzustufenden Instituten mit einer Mitarbeiterzahl in kleiner oder mittlerer Größenordnung zu eher kleinen Einheiten in der 2nd line of defence mit erhöhtem Koordinationsaufwand und infolgedessen tendenziell zu einer Schwächung der 2nd line of defence-Funktionen allgemein und der Compliance-Funktion im Besonderen führen.

Es sind unseres Erachtens auch keine, wie von Ihnen aufgeführten Interessenkonflikte bei der Tätigkeit hier aufgeführter Bereiche erkennbar. Im Gegenteil besteht ein Zusammenhang der

Bereiche, die von gegenseitigen Ergebnissen ihrer Risikominderung im Haus profitieren können, sodass unnötig eine Aufspaltung herbeigeführt würde. Diese Aufspaltung führt zu mehr Schnittstellen und Abstimmungsbedarf, sodass eine einhergehende Komplexitätserhöhung im Ergebnis zu einer Risikoerhöhung führt.

Aus diesem Grund hat es uns stark verwundert, dass Sie mit der vorliegenden Novelle genau diesen natürlichen, unserer Meinung nach auch sehr sinnvollem Trend der Verzahnung der Disziplinen mit der Kommentierung der Textziffer 4 des AT 4.4.2 komplett entgegentreten wollen. Wir sehen – wie vorstehend dargestellt – einen sehr großen Vorteil im Zusammenführen der unabhängigen Funktionen.

Die Schaffung eines Compliance-Bereichs, in dem die verschiedenen sektoralen Compliance-Funktionen organisatorisch zusammengeführt sind, mündet in einer engeren Zusammenarbeit der Compliance-Funktionen untereinander. Abstimmungswege werden hierdurch kürzer, Schnittstellen über Bereichsgrenzen hinweg entfallen, womit für die Compliance-Organisation erhebliche Synergien gehoben werden können. Einfach gesagt: kurze Wege und einheitliche Betrachtungen führen zu einem besseren Ergebnis. Dies führt aber auch dazu, dass das Thema „Compliance“ nicht aus verschiedenen „Ecken“ eines Instituts an die operativ tätigen Geschäftsbereiche herangetragen wird, sondern ein zentraler Bereich in diesem Kontext wahrgenommen wird. So können sich auch die 1st Line-Funktionen an einen Adressaten im Institut wenden, wenn Bedarf für Beratung in Compliance-Fragen besteht.

Bezieht man ergänzend Aspekte der Compliance-Kultur in die Betrachtung mit ein, sollten in einem Institut die Compliance-Funktionen – soweit möglich – eng miteinander verzahnt und nicht in kleinen Einheiten im Institut verstreut, geradezu versteckt werden. Bei einer „zersplitterten“ Compliance-Organisation fällt es Mitarbeitern im Zweifel schwer, den für ihre Fragestellung richtigen „Compliance-Ansprechpartner“ auszumachen. Dies führt insgesamt nicht zu einer positiven Wahrnehmung von Compliance und birgt dann die Gefahr, dass mangels Sensibilität und Kenntnis Verstöße gegen externe aber auch institutsinterne Vorgaben auftreten.

Zur Funktion des Datenschutzbeauftragten: Artikel 38 DSGVO sieht für die Stellung des Datenschutzbeauftragten im Unternehmen konkrete Anforderungen an die Weisungsungebundenheit und die direkte Berichtslinie an die Geschäftsleitung vor. Insbesondere Geldwäsche- und Datenschutzbeauftragte verfolgen in gewissen Themen unterschiedliche Zielrichtungen, die vereinfacht ausgedrückt als „Datensammlung vs. Datensparsamkeit“ bezeichnet werden können. So wäre nach unserer Auffassung lediglich eine organisatorische Anbindung des Datenschutzbeauftragten an einen Compliance-Bereich möglich. Eine disziplinarische Anbindung – insbesondere auch verbunden mit einer Weisungsgebundenheit – ist unseres Erachtens vor dem Hintergrund von Artikel 38 DSGVO ausgeschlossen.

Vor dem Hintergrund der vorstehenden Ausführungen regen wir daher an, die Passage in AT 4.4.2 Tz. 4 (Erläuterungen) ersatzlos zu streichen. Denn unserer Einschätzung nach greift die Aufsicht durch die restriktiven Ausführungen zudem in die unternehmerische Freiheit der Institute ohne Rechtsgrund und erkennbare Vorteile ein.

Art. 4.4.2 TZ 7 Ausschüsse des Aufsichtsorgans

7	Die Compliance-Funktion hat mindestens jährlich sowie anlassbezogen der Geschäftsleitung über ihre Tätigkeit Bericht zu erstatten. Darin ist auf die Angemessenheit und Wirksamkeit der Regelungen zur Einhaltung der wesentlichen rechtlichen Regelungen und Vorgaben einzugehen. Ferner hat der Bericht auch Angaben zu möglichen Defiziten sowie zu Maßnahmen zu deren Behebung zu enthalten. Die Berichte sind auch an das Aufsichtsorgan und die Interne Revision weiterzuleiten.	**Ausschüsse des Aufsichtsorgans** Adressat der Berichterstattung sollte grundsätzlich jedes Mitglied des Aufsichtsorgans sein. Soweit das Aufsichtsorgan Ausschüsse gebildet hat, kann die Weiterleitung der Informationen auch auf einen Ausschuss beschränkt werden. Voraussetzung dafür ist, dass ein entsprechender Beschluss über die Einrichtung des Ausschusses besteht und der Vorsitzende des Ausschusses regelmäßig das gesamte Aufsichtsorgan informiert. Zudem ist jedem Mitglied des Aufsichtsorgans weiterhin das Recht einzuräumen, die an den Ausschuss geleitete Berichterstattung einsehen zu können.

Wir begrüßen eine entsprechende Klarstellung – hierdurch wird ein in der Praxis immer wieder auftauchendes Problem geregelt. Gesamt-Verteilerkreise und Gesamt-Verantwortung des Kontrollorgans sollten zusammengeführt werden.

Zu AT 9 Auslagerungen

Finanzdienstleistungsaufsicht

AT 9 Auslagerung

1	Eine Auslagerung liegt vor, wenn ein anderes Unternehmen mit der Wahrnehmung solcher Aktivitäten und Prozesse im Zusammenhang mit der Durchführung von Bankgeschäften, Finanzdienstleistungen oder sonstigen institutstypischen Dienstleistungen beauftragt wird, die ansonsten vom Institut selbst erbracht würden. Zivilrechtliche Gestaltungen und Vereinbarungen können dabei das Vorliegen einer Auslagerung nicht von vornherein ausschließen.	**Sonstiger Fremdbezug von Leistungen** Nicht als Auslagerung im Sinne dieses Rundschreibens zu qualifizieren ist der sonstige Fremdbezug von Leistungen. Hierzu zählt zunächst der einmalige oder gelegentliche Fremdbezug von Gütern und Dienstleistungen. Ebenso erfasst werden Leistungen, die typischerweise von einem beaufsichtigten Unternehmen bezogen und aufgrund tatsächlicher Gegebenheiten oder rechtlicher Vorgaben regelmäßig weder zum Zeitpunkt des Fremdbezugs noch in der Zukunft vom Institut selbst erbracht werden können. Dazu zählen (z. B.

Uns ist aufgefallen, dass nunmehr in den MaRisk ein weiterer Begriff – wahrscheinlich durch die Übernahme aus den EBA-Leitlinien zu Auslagerungen (EBA/GL/2019/02) – Einzug gefunden hat. Der Begriff der „Auslagerungsvereinbarung“ ist bisher nicht in den MaRisk verwendet und schafft – sofern er neben dem Begriff des Auslagerungsvertrages stehen bleibt – unseres Erachtens keine sinnstiftende Klarheit. Insoweit regen wir an, die Begrifflichkeit – je nach Zusammenhang – auf „Auslagerung“ und „Auslagerungsvertrag“ zu vereinheitlichen.

Zu AT 9 TZ 1 (Erläuterungen)

Die Übernahme der in den EBA-Leitlinien zu Auslagerungen (EBA/GL/2019/02) genannten Beispiele für sonstige Fremdbezüge begrüßen wir ausdrücklich. Dass die Aufzählung zudem weiter beispielhaft ist, halten wir insbesondere auch im Sinne einer praktischen Umsetzung für angemessen.

Wir begrüßen weiterhin die Übernahme der Anmerkungen aus dem Fachgremium MaRisk aus März 2018 hinsichtlich des Betriebs von Software durch einen externen Dritten. Wir bedauern dagegen, dass die weiteren Klarstellungen hinsichtlich der Wartung von Software aus demselben Termin des Fachgremiums MaRisk nicht Eingang in die Erläuterungen gefunden haben. Wir bitten, diese weiteren Klarstellungen zur Wartungs-Thematik mit in den Text aufzunehmen.

Zu AT 9 TZ 2 (Erläuterungen)

Wir regen die Streichung der Betrachtung „politischer Risiken“ an, auch wenn es sich um die Abbildung von Tz. 68 lit. d der EBA-Leitlinien zu Auslagerungen handelt. „Politische Risiken“

ist ein unbestimmter Begriff und es ist fraglich, anhand welcher Kriterien politische Risiken betrachtet werden sollen. Wenn nach Auffassung der BaFin dieser Aspekt in den Erläuterungen verbleiben sollte, bedürfte er unseres Erachtens näherer Erläuterung und Konkretisierung. Welchen Faktoren wären für die Beurteilung heranzuziehen, wären nach Auffassung der BaFin hier z. B. Governance Indicators der Weltbank heranzuziehen? Oder sollte das Vorhandensein von Gesetzen zum Datenschutz, zum Insolvenzrecht oder Prozessrecht zu betrachten sein? Auch in diesem Fall anhand welcher Erkenntnisquellen sollte dies beurteilt werden? Insoweit handelt es sich bei diesem Kriterium um einen Risikofaktor, bei dem tatsächlich nur schwerlich ein Erkenntnisgewinn für etwaige Steuerungs- und Risikomitigierungsmaßnahmen generiert werden kann.

Weiterhin halten wir eine Streichung der Beurteilung von „Maßnahmen zur Steuerung und Minderung der Risiken“ für angemessen. Denn die Risikoanalyse erfolgt initial vor Eingehung einer Auslagerung, insoweit in einem Stadium, in dem zunächst die Brutto-Risiken analysiert werden. Auch im weiteren Verlauf einer Auslagerung und im Rahmen der regelmäßigen Aktualisierung sind die Bruttorisiken zu analysieren, deren Ergebnisse dann in einer Aktualisierung der Steuerungsmaßnahmen münden. Insoweit ist die Abfrage von Maßnahmen zur Steuerung und Minderung von Risiken in der Risikoanalyse nicht korrekt verortet. Vielmehr ist eine Konnektivität zwischen Umfang, Intensität etc. der Steuerungsmaßnahmen zum Ergebnis der Risikoanalyse herzustellen. Dies wird richtigerweise auch in Tz. 2 mit der Anforderung „Die Ergebnisse der Risikoanalyse sind in der Auslagerungs- und Risikosteuerung zu beachten.“ formuliert.

Zu AT 9 TZ 4 (Erläuterungen)

An dieser Stelle regen wir an, für die Institute klarzustellen, in welchem Umfang jeweils durch das Institut sicherzustellen ist, dass eine Auslagerungsunternehmen nach dem Recht seins Sitzlandes ggfs. entsprechende Erlaubnisse bzw. Registrierungen hat. Nicht alle Aufsichtsbehörden – insbesondere außerhalb des EU-/EWR-Raumes – verfügen über allgemein zugängliche Register, die eine entsprechende Recherche ermöglichen. Insoweit wäre eine Öffnung der Anforderungen unsererseits begrüßenswert, die das Anfordern von Nachweisen beim Auslagerungsunternehmen als operative Möglichkeit aufnehmen.

Vergleichbares gilt für den Nachweis der Beaufsichtigung durch zuständige Aufsichtsbehörden in Drittstaaten. Hier regen wir an, dass es den Instituten ermöglicht wird, sich dies durch entsprechende vertragliche Regelungen zusichern zu lassen.