Mindestanforderungen an das Risikomanagement (MaRisk)

Protokoll zur Sondersitzung des Fachgremiums MaRisk am 15.03.2018 in Bonn (BaFin)
Thema: Auslagerung

1. Begrüßung

Die Aufsicht begrüßt die Teilnehmer und gibt einen kurzen Überblick über die Themen, die in der Sondersitzung behandelt werden sollen.

2. Abgrenzung Auslagerung von Fremdbezug – Reichweite des Auslagerungsbegriffs

Die Aufsicht fasst ihre Sichtweise hinsichtlich der Frage zusammen, wann der Anwendungsbereich des § 25b KWG eröffnet ist und wie sich Fremdbezug und Auslagerung voneinander abgrenzen. Es wird darauf hingewiesen, dass im Gesetzeswortlaut die wesentlichen Kriterien zur Unterscheidung enthalten sind. Eine Auslagerung liegt dann vor, wenn Aktivitäten und Prozesse Bestandteil von Bankgeschäften, Finanzdienstleistungen (siehe § 1 KWG) oder sonstigen institutstypischen Dienstleistungen sind und ein anderes Unternehmen mit der Wahrnehmung dieser Aktivitäten und Prozesse beauftragt wird, die ansonsten von dem Institut selbst erbracht würden. Darüber hinaus wird seitens der Aufsicht klargestellt, dass Fremdbezug nicht gleichbedeutend mit dem Nichtvorliegen eines Risikos ist. Auf der anderen Seite begründet das Vorhandensein eines operationellen Risikos per se noch keine Auslagerung, sofern der Anwendungsbereich der gesetzlichen Regelung des § 25b KWG nicht eröffnet ist.

Im Weiteren wird die Unterscheidung von „wesentlichen“ und „unwesentlichen“ Auslagerungen diskutiert. Mittels Risikoanalyse ist zunächst erst einmal zu prüfen, welche Risiken mit der geplanten Maßnahme überhaupt verbunden sind und ob diese Risiken in einer Gesamtschau wesentlich oder unwesentlich sind. Dabei können unterschiedlichste Aspekte eine Rolle spielen (konkreter Gegenstand der Auslagerung, Auswirkungen der Maßnahme auf das Institut, Ort der Leistungserbringung, Komplexität der geplanten Maßnahme, Eignung potenzieller Dienstleister etc.). Schließlich wird mittels Risikoanalyse - quasi als deren Ausfluss - auch festgestellt, ob eine Auslagerung als wesentlich oder unwesentlich anzusehen ist. Im Ergebnis wird sich das Institut mithilfe der Risikoanalyse der Risiken durch die Auslagerung bewusst.

Die Aufsicht weist darauf hin, dass die *CEBS-Guidelines on Outsourcing (CEBS-Guidelines)*, die am 14. Dezember 2006 veröffentlicht wurden, über § 25b KWG in deutsches Recht überführt wurden, der insbesondere durch AT 9 MaRisk, letztmalig in deren Novelle 2017, konkretisiert wird. Die zukünftigen *EBA-Guidelines on Outsourcing arrangements (EBA-Guidelines)*, die sich aktuell im Entwurfsstadium befinden, sollen ebenfalls in den MaRisk Berücksichtigung finden. Die ersten Entwürfe deuten aus Sicht der Aufsicht darauf hin, dass die neuen Leitlinien deutlich umfangreicher und detaillierter als ihre Vorgängerversion ausfallen werden und die EBA nach dem bisherigen Kenntnisstand noch in diesem Jahr plant, diese *EBA-Guidelines* zu verabschieden.

Aus dem Teilnehmerkreis wird die Frage nach der Bedeutung des Satzes in AT 9 Tz. 1 MaRisk aufgeworfen: „Zivilrechtliche Gestaltungen und Vereinbarungen können dabei das Vorliegen einer Auslagerung nicht von vornherein ausschließen.“ Die Aufsicht erläutert dazu, dass der Hintergrund

für diesen Passus – der im Übrigen wortgleich auch in den MaComp zu finden ist - die Tatsache ist, dass bestimmte rechtliche Fallgestaltungen (z.B. Arbeitnehmerüberlassungen) nicht per se vom Anwendungsbereich des § 25b KWG ausgeschlossen werden können. Auf die formalrechtliche Hülle kommt es daher nicht an, sondern „lediglich“ auf die konkrete materielle Ausgestaltung und Bedeutung im Einzelfall. Die Aufsicht wird daher auch weiterhin die aus ihrer Sicht bewährte Einzelfallbetrachtung fortführen und keine pauschalen Ausnahmen vom § 25b KWG i.V.m. AT 9 MaRisk schaffen. Eine Ausweitung von Auslagerungstatbeständen ist damit keinesfalls intendiert, diese sind ohnehin durch § 25b KWG relativ klar umrissen (siehe oben).

3. Mehrmandantendienstleister und gruppen- / verbundinterne Auslagerungen

Die Behandlung von Mehrmandantendienstleistern wird insbesondere hinsichtlich der Aspekte Verantwortung (der Geschäftsleiter; § 25a Abs. 1 Satz 2 KWG) und Berichtswesen diskutiert. Die Aufsicht weist darauf hin, dass die Problematik der Mehrmandantendienstleister im Rahmen dieser Sitzung nicht abschließend geklärt werden kann.

Hinsichtlich des Aspektes Verantwortung wird von einzelnen Teilnehmern die Schwierigkeit herausgestellt, dass der Mehrmandantendienstleister aufsichtsrechtlich nicht die Verantwortung trägt, da gegenüber der Aufsicht die Geschäftsleiter des auslagernden Instituts für die Ordnungsmäßigkeit der Aktivitäten und Prozesse, folglich auch für damit zusammenhängende Mängel verantwortlich sind. Es existiert keine Rechtsgrundlage im KWG, um den Mehrmandantendienstleister direkt in die Pflicht zu nehmen. Da eine Aufsicht über einen Mehrmandantendienstleister in der Praxis nicht vorgesehen ist (mangels Rechtsgrundlage), werden Feststellungen, die faktisch die Ebene des Mehrmandantendienstleisters betreffen, in den Prüfungsbericht des jeweiligen Instituts aufgenommen. Folglich ist das Institut in der Pflicht, die Mängel unter Einbeziehung des Mehrmandantendienstleisters zu beheben bzw. darauf hinzuwirken, dass die Mängel vom Dienstleister beseitigt werden, was wiederum entsprechende Überwachungshandlungen zur Leistungserbringung und zur Einhaltung rechtlicher Vorgaben voraussetzt. Der Aufsicht ist bewusst, dass dies in einzelnen Fällen die Institute vor besondere Herausforderungen stellt, vor allem dann, wenn der Einfluss eines einzelnen Instituts auf den Mehrmandantendienstleister gering ist. Aufgrund der aktuellen Rechtslage, die im Übrigen mit aktuellen europäischen und internationalen Vorgaben korrespondiert, ist dies aber kaum zu vermeiden.

Für Verbundinstitute ist es zudem immer zu empfehlen, dass das Institut über den Verbund etwaige Mängel an den Mehrmandantendienstleister heranträgt. Dies entspricht nach aufsichtlichem Kenntnisstand der bisherigen Praxis.

Hinsichtlich des Aspektes Berichtspflicht wird von den Teilnehmern die Problematik erläutert, dass Rechenzentren sehr umfangreiche Berichte an die Institute weitergeben, die von diesen aufwendig analysiert werden müssen. Die Aufsicht stellt in diesem Zusammenhang klar, dass sie nicht das Problem der adressatengerechten Berichterstattung lösen kann, allerdings können nach Ansicht der Aufsicht zentrale Interpretationshilfen für die Analyse der Berichte von den Instituten genutzt werden. Darüber hinaus ist denkbar, dass sich insbesondere verbandsgeprüfte Institute aufgrund ihrer grundsätzlich homogeneren Struktur einer zentralen verbandsseitigen Auswertung bedienen, wo dies sinnvoll möglich ist.

Bei der Behandlung internationaler Gruppen merkt die Aufsicht an, dass eine vollständige Auslagerung hinsichtlich bestimmter Bereiche / Funktionen in Drittstaaten, insbesondere solche mit steuernder Funktion (Geschäftsabschließende Bereiche, Kontroll- und Überwachungsfunktionen) schwer vorstellbar ist. Sie weist darauf hin, dass sich die EZB im Rahmen der Brexitdiskussion bereits dahingehend positioniert hat, dass eine vollständige Auslagerung der Kontrollfunktionen in Drittstaaten nicht möglich sein soll. Vorstellbar ist jedoch, dass Teile dieser Funktionen (einzelne Prozesse oder Aktivitäten) an Dienstleister in Drittstaaten ausgelagert werden können.

4. Auslagerung Kontrollfunktionen/Kernbankbereiche

AT 9 Tz. 5 MaRisk schränkt die Auslagerung der besonderen Funktionen anhand bestimmter Kriterien ein. Demnach ist „eine vollständige Auslagerung der besonderen Funktionen Risikocontrolling-Funktion, Compliance-Funktion oder Interne Revision […] lediglich für Tochterinstitute innerhalb einer Institutsgruppe zulässig, sofern das übergeordnete Institut Auslagerungsunternehmen ist und das Tochterinstitut sowohl hinsichtlich seiner Größe, Komplexität und dem Risikogehalt der Geschäftsaktivitäten für den nationalen Finanzsektor als auch hinsichtlich seiner Bedeutung innerhalb der Gruppe als nicht wesentlich einzustufen ist.“ Die Teilnehmer bewerten den Umstand, dass nur das übergeordnete Institut Auslagerungsunternehmen sein darf, als schwierig.

Des Weiteren besagt AT 9 Tz. 5 MaRisk, dass „eine vollständige Auslagerung der Compliance-Funktion oder der Internen Revision […] ferner nur bei kleinen Instituten möglich [ist], sofern deren Einrichtung vor dem Hintergrund der Institutsgröße sowie der Art, des Umfangs, der Komplexität und des Risikogehalts der betriebenen Geschäftsaktivitäten nicht angemessen erscheint.“ Die Teilnehmer fragen nach, wie ein „kleines Institut“ definiert ist. Die Aufsicht stellt klar, dass sie auch in Zukunft keine starre – quantitative – Abgrenzung hierzu vorgeben wird, um den Handlungsspielraum in der Aufsichtspraxis nicht von vornherein unnötig einzuschränken. Hinsichtlich der Compliance-Funktion wird seitens der Teilnehmer angemerkt, dass die Beschränkung auf „kleine“ Institute für Verbundinstitute zu streng ist, da verbundinterne Auslagerungen auch für mittelgroße Institute angemessen sein können.

Die Frage der Teilnehmer nach einer Definition für Kernbankbereiche beantwortet die Aufsicht dahingehend, dass eine pauschale Definition nicht gegeben werden kann, da sie vom Geschäftsmodell des jeweiligen Instituts abhängt. Die Relevanz kann sich z.B. im Hinblick auf den Anteil am Gesamtertrag und Gesamtrisiko ergeben. Bei Universalbanken, Sparkassen oder Genossenschaftsbanken wird zum Beispiel die Kreditbearbeitung als Kernbankbereich angesehen. Oft können die dazugehörigen IT-Prozesse nicht von der Geschäftsseite getrennt gesehen werden. So gesehen ist grundsätzlich auch die IT-Unterstützung solcher Aktivitäten und Prozesse als Bestandteil des Kernbankbereiches anzusehen. Demgegenüber ist aber zum Beispiel nicht jeder noch so kleine Teil eines erlaubnispflichtigen Geschäfts i. S. von § 1 Abs. 1 KWG als Kernbankbereich einzustufen, auch hier kommt es auf das Geschäftsmodell des Instituts an.

Die Teilnehmer werfen die Frage auf, ob eine Auslagerung vorliegt, wenn die Revision im Institut auf Spezialisten der Konzernrevision zurückgreift, um bestimmte Sachverhalte besser untersuchen zu können. Die Aufsicht merkt an, dass es sich in diesem Fall - unter dem Vorbehalt, dass der Einzelfall genau zu prüfen ist - um eine Auslagerung gem. AT 9 Tz. 1 MaRisk handelt. Ob diese wesentlich oder unwesentlich ist, hängt vom konkreten Einzelfall ab.

In der Erläuterung zu AT 9 Tz. 2 MaRisk kommt der Begriff „Auslagerungen von erheblicher Tragweite“ vor. Die Teilnehmer fragen nach dem Unterschied zwischen der „Auslagerung von erheblicher Tragweite“ und der „wesentlichen Auslagerung“. Die „erhebliche Tragweite“ zielt nach Erläuterung der Aufsicht auf das Risikobewusstsein des auslagernden Instituts ab, d.h. eine solche Auslagerung soll gut überlegt sein. Im Vorfeld entsprechender Auslagerungsmaßnahmen sollte zum Beispiel über Überwachungsmechanismen, die Komplexität einer eventuellen Zurückholung der ausgelagerten Funktion und die Abhängigkeit des Instituts mit Blick auf das Kernbankgeschäft kritisch reflektiert werden. Bei teilweisen Auslagerungen von besonderen Funktionen oder Kernbankbereichen ist als Ergebnis der Risikoanalyse eine Einstufung als nicht wesentliche Auslagerung durchaus möglich.

5. Abgrenzung Auslagerung von Fremdbezug – Software / IT-Dienstleistungen

Diskutiert wird seitens der Mitglieder des Fachgremiums, ob der Betrieb von Software in einer Cloud einen Auslagerungstatbestand darstellt. Der Betrieb von Software in einer Cloud ist immer dann als Auslagerung einzustufen, wenn die Cloud nicht vom Institut selbst erstellt worden ist, nicht unter eigener Kontrolle des Instituts steht sowie Software betrieben wird, die zur Durchführung von Bankgeschäften, Finanzdienstleistungen oder sonstigen institutstypischen Dienstleistungen genutzt wird. Das ist jedenfalls dann der Fall, wenn sie für die Risikosteuerung eingesetzt wird oder für die Durchführung von bankgeschäftlichen Aufgaben von wesentlicher Bedeutung ist. D.h., beim externen Betrieb gelten die gleichen Abgrenzungskriterien für Software wie bei den zuvor in AT 9 Tz. 1 Erl. genannten Unterstützungsleistungen.

Die Aufsicht stellt darüber hinaus klar, dass zu berücksichtigen ist, wofür eine Software verwendet wird. Wenn die Nutzung der Software zum Beispiel von wesentlicher Bedeutung für die Durchführung von Bankgeschäften ist, gilt dies auch für die entsprechenden Unterstützungsleistungen. Diese Unterstützungsleistungen (und nur diese, nicht der Bezug der Software als solche, unabhängig davon, ob die Software gekauft wurde oder eine Lizenz zur Nutzung der Software vorliegt) sind gemäß AT 9 Tz. 1 Erläuterung MaRisk als Auslagerung einzustufen.

Im Zuge der Diskussion kommt die Frage nach der Bedeutung des Begriffs „Wartung“ im Sinne der MaRisk auf. Die Wartung einer Software schließt die Behebung von Fehlern des Programms mit ein. Wenn das Institut die gelieferten „Patches“ vor dem Einspielen in das System selbst testet, handelt es sich nicht zwangsläufig um eine Auslagerung, da das Institut sich eigenständig ein Bild zu den erweiterten Funktionen oder Fehlerbehebungen macht und eigenständig die Funktionsweise im eigenen System prüft. Wenn ein Dritter die Software wartet, ohne dass von dem Institut die Neuerungen im Rahmen der Wartung selbst getestet werden, liegt hingegen eine Auslagerung vor.

6. Auslagerungssteuerung

a. Risikoanalyse:

Die Aufsicht stellt zunächst die Zielrichtung der in den MaRisk geforderten Risikoanalyse dar. Mittels Risikoanalyse ist im ersten Schritt zu prüfen, welche Risiken mit der geplanten Maßnahme überhaupt verbunden sind. In einer Gesamtschau wird anschließend entschieden, ob diese Risiken wesentlich oder unwesentlich sind. AT 9 Tz. 2 MaRisk mit den dazugehörigen Erläuterungen ist so zu verstehen, dass, auch wenn alle Auslagerungen als wesentlich eingestuft worden sind, eine aussagefähige und

nachvollziehbare Risikoanalyse durchgeführt werden muss. Ein hoher Standardisierungsgrad ist für eine Risikoanalyse sicherlich von Vorteil, allerdings muss auch gewährleistet sein, dass eine individuelle Beurteilung der jeweiligen Situation erfolgen kann.

Der Turnus für die Durchführung einer Risikoanalyse bzw. dessen Überprüfung wird in den MaRisk nicht weiter spezifiziert, ist für wesentliche und unwesentliche Auslagerungen naturgemäß aber differenziert zu betrachten. Als Richtschnur hat sich in der Aufsichtspraxis für wesentliche Auslagerungen eine jährliche Analyse und für unwesentliche Auslagerungen ein Turnus von drei Jahren etabliert. Ein Abweichen davon im Einzelfall ist nicht ausgeschlossen.

In eine Risikoanalyse ist die Möglichkeit einer Weiterverlagerung einzubeziehen. Dies wird auch durch die diesbezüglichen Anforderungen an die Ausgestaltung des Auslagerungsvertrags bei wesentlichen Auslagerungen deutlich (Zustimmungsvorbehalte bei Weiterverlagerungen oder Festlegung konkreter Kriterien, wann diese möglich sein soll). Die Risikoanalyse ist vom Institut bei einer Weiterverlagerung durch den Dienstleister zu überprüfen, da sich die Risikolage geändert haben könnte.

Die Risikobewertung gemäß Tz. 53 BAIT ist nicht gleich zu setzen mit der Risikoanalyse gemäß AT 9 Tz. 2 MaRisk. Sie muss für jeden IT-Fremdbezug erfolgen, nachvollziehbar abgefasst sein und kann weniger detailliert, strukturiert und umfangreich ausfallen als eine Risikoanalyse nach AT 9 Tz. 2 MaRisk. Sofern ein Institut die Risikoanalyse auch für jeden IT-Fremdbezug durchführen möchte, so steht ihm dies selbstverständlich frei. Bei der Risikobewertung von Fremdbezügen gemäß BAIT kann auf die Schutzbedarfsklassen Bezug genommen werden.

b. Auslagerungsvertrag:

Die Aufsicht macht zudem deutlich, dass es keinen Bestandsschutz für bestehende Auslagerungsverträge gibt. Diese sind im Zeitverlauf an die neuen Anforderungen der MaRisk anzupassen.

Seitens der Aufsicht werden keine Vorgaben gemacht, wann der Dienstleister wegen einer Schlechtleistung zu wechseln ist. Sowohl die Entscheidung über einen Anbieterwechsel als auch die Aufstellung eines Maßnahmenkatalogs für Schlechtleistungen obliegen dem Institut.

c. Weiterverlagerungen:

Die Aufsicht stellt auf Nachfrage von Teilnehmern klar, dass die erweiterten Anforderungen gemäß AT 9 MaRisk für wesentliche Auslagerungen auch nur für unter Risikogesichtspunkten wesentliche Weiterverlagerungen gelten.

d. Zentrales Auslagerungsmanagement:

Die Einrichtung eines zentralen Auslagerungsmanagements ist abhängig davon, ob Institute eine hohe Anzahl von Auslagerungen, eine hohe Komplexität der Auslagerungen und einen hohen Abstimmungsaufwand aufweisen. Es gibt diesbezüglich jedoch keine festgelegten Grenzen. Die Kriterien müssen institutsindividuell definiert und bewertet werden. Die Regelung zur Einrichtung zielt insgesamt eher auf größere Institute ab, da davon auszugehen ist, dass bei kleinen Instituten eine Koordinierung und ein Überblick hinsichtlich der Auslagerungen leichter möglich sind.

Die Aufsicht stellt im Laufe der Diskussion klar, dass ein Auslagerungsmanagement nicht bei der Internen Revision anzusiedeln ist. Eine eigenständige Organisationseinheit wird nicht gefordert. Die Dokumentationsanforderungen im Auslagerungsmanagement sollen zudem nur einen Überblick (z.B. durch ein Register) gewährleisten. Es ist nicht gefordert, die Dokumentation zu den einzelnen Auslagerungen zusätzlich zu den Dokumentationen der zuständigen Geschäftsbereiche zu doppeln. Die Aufsicht weist des Weiteren darauf hin, dass nicht pauschal festgelegt werden kann, dass ein rein zentrales Auslagerungsmanagement auf Gruppenebene ausreicht. Hier ist der Einzelfall zu prüfen.