Dr. Patrik Buchmüller / Oliver Rambock

„Was kommt da?“-Reihe

EBA Leitlinien zu Auslagerungen

Arbeitsbuch zur Umsetzung der Anforderungen aus den EBA Leitlinien vom 25. Februar 2019

DEMOVERSION

MARISKACADEMY

Dr. Patrik Buchmüller / Oliver Rambock

EBA Leitlinien zu Auslagerungen

Arbeitsbuch zur Umsetzung der Anforderungen aus den EBA Leitlinien vom 25. Februar 2019

1. Auflage

in der Reihe:

MARISK ACADEMY – Was kommt da?

www.marisk.academy

 r-alpha LABS GmbH
Am Alten Berg 32
64342 Seeheim-Jugenheim

www.r-alpha.de
kontakt@r-alpha.de

Inhalt

1 Vorwort

Auslagerungen stellen für Kreditinstitute nach wie vor eine effektive Möglichkeit dar, Kosten einzusparen oder neue Technologien schnell für sich nutzbar zu machen.

Allerdings sind mit Auslagerungen auch eine Vielzahl von Risiken verbunden, die es zu identifizieren, zu bewerten und angemessen zu steuern gilt.

Bereits mit dem Mindestanforderungen an das Risikomanagement (MaRisk) sowie den Bankaufsichtlichen Anforderungen an die IT (BAIT) hat die deutsche Finanzdienstleistungsaufsicht Anforderungen an Auslagerungen von Kreditinstituten formuliert.

Entsprechende Anforderungen bestehen auch in einer Reihe anderer Länder der EU.

Mit den EBA Leitlinien zu Auslagerungen vom 25. Januar 2019 soll nunmehr – ausgehend von den CEBS Leitlinien aus 2006 – ein einheitlicher europäischer Regelungsrahmen geschaffen werden.

Das vorliegende Arbeitsbuch möchte allen Verantwortlichen eine Arbeitshilfe bei der Umsetzung der Anforderungen aus den EBA Leitlinien sein.

Bei seiner Erstellung haben wir sehr viel Wert auf eine umfassende und detaillierte Darstellung der einzelnen Anforderungen gelegt. Nichtsdestotrotz können wir keine Garantie für die Vollständigkeit und Richtigkeit der gemachten Angaben gewähren.

Auch eine Haftung für Umsetzungen, die auf den Inhalten aus diesem Arbeitsbuch basieren, können wir ausdrücklich nicht übernehmen.

Wir hoffen, Ihnen dennoch einen spürbaren Mehrwert liefern zu können, um Sie dem wohlverdienten Erfolg Ihres Umsetzungsprojektes ein gutes Stück näher zu bringen.

In diesem Sinne wünschen wir Ihnen gutes Gelingen.

Es grüßen Sie im Juli 2019,

Patrik Buchmüller & Oliver Rambock

2 Arbeiten mit dem Arbeitsbuch

Dieses Arbeitsbuch kann als Download im PDF-Format über die MARISK ACADEMY unter

www.marisk.academy

bezogen werden.

Neben diesem Arbeitsbuch enthält der Download noch eine Checkliste im MS Excel-Format, die alle Anforderungen auf Textziffern-Ebene behandelt.

Zur Dokumentation Ihrer Umsetzung empfehlen wir die Nutzung dieser Checkliste. Neben dem englischen Originaltext finden Sie dort auch die deutsche Übersetzung vom Juni 2019.

Zur vollständigen Abdeckung aller regulatorischen Anforderungen zu Auslagerungen haben wir in der Checkliste auch die aktuellen Vorgaben der MaRisk (AT 9 in der Version vom 27.10.2017) und der BAIT (Abschnitt II.8 in der Fassung vom 14.09.2018) zu diesem Themenbereich integriert.

Weitere Hinweise zum Einsatz der Checkliste finden Sie in der MS-Excel Datei auf dem Arbeitsblatt „Beschreibung der Tabellenfelder“.

Kommen wir nun zum Einsatz des vorliegenden Arbeitsbuchs.

Da es sich um ein **Arbeits**buch handelt, haben Sie die Möglichkeit umfangreiche Notizen direkt im Buch vorzunehmen.

Zu diesem Zweck empfiehlt sich ein Ausdruck der PDF-Datei und das Abheften in einem Ringordner.

Aber bitte dann nicht gleich im hintersten Aktenschrank Ihres Büros wegschließen, auch wenn die Versuchung groß sein sollte! 😉

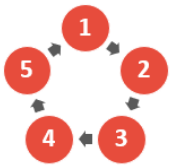
Beachten Sie bitte, dass wir Ihnen das Arbeitsbuch in **zwei Druckversionen** zur Verfügung stellen. Auf die Unterschiede beider Versionen gehen wir am Ende dieses Abschnitts ein.

Das Arbeitsbuch in ausgedruckter Form soll unmittelbar der Arbeit an Ihrem Umsetzungsprojekt dienen im Gegensatz zu den üblichen Handbüchern, die eher Hintergrundwissen zum Regelungskontext liefern.

Wie genau das funktioniert, wollen wir Ihnen im Folgenden erläutern.

Zunächst aber noch ein paar Worte zur Umsetzung regulatorischer Anforderungen in den Instituten im Allgemeinen.

Unserer Erfahrung nach ist es so, dass sich beim Umsetzen neuer oder überarbeiteter Normen, dem Regulatory Lifecycle Management wie wir es nennen, die Umsetzungsverantwortlichen den immer gleichen Herausforderungen gegenüberstehen und Antworten auf die immer gleichen Fragestellungen finden müssen:



Regulatory Lifecycle Management

Aufgabenstellung	Fragestellung
❶ Überblick verschaffen	Was kommt da?
❷ relevante Anforderungen identifizieren	
❸ Handlungsbedarf klären	
❹ Anforderungen optimal umsetzen	Wie mache ich das?
❺ nichts vergessen	An alles gedacht?

Abbildung 1: Regulatory Lifecycle Management

Zunächst gilt es, die Frage „Was kommt da?“ zu beantworten, d.h. sich einen Überblick über die Zielsetzung, die Struktur sowie die Schwerpunktthemen der Norm zu verschaffen.

Dann stellt sich die Frage, welche Anforderungen speziell für Ihr Haus relevant sind.

Wenn eine Anforderung relevant ist, besteht hier überhaupt Handlungsbedarf?

Und wenn ja, in welchem Umfang und wie sieht eine optimale Umsetzung aus?

Damit wären wir bei der Frage „Wie mache ich das?“ angelangt. Am besten optimal lautet hier die ideale Antwort.

Mit optimal meinen wir eine Umsetzung, die möglichst viel von dem, was bereits vorhanden ist, nutzt und bei Bedarf intelligent weiterentwickelt.

Häufig geht es bei aktuellen regulatorischen Initiativen um Anforderungen, die in weiten Teilen gar nicht wirklich neu und somit bereits in den Instituten umgesetzt sind. Allerdings bisher ohne den regulatorischen Fokus.

Sicher wird niemand bestreiten, dass sich Institute bereits heute intensiv mit der Auslagerung von Systemen, Prozessen oder Funktionen beschäftigen.

Neu ist, dass die Regulatoren das Thema nun stärker aufgreifen und Institute in diesem Bereich mit intensiveren Überprüfungen rechnen müssen.

Gleiches gilt beispielsweise auch für die Informationstechnologie und deren Sicherheit, die in den BAIT oder den EBA Leitlinien zum Management von IKT- und Sicherheitsrisiken einer Regulierung unterworfen werden.

In diesen Fällen gilt es, die bereits bestehende Ablauforganisation (Arbeitsabläufe und Methoden) angemessen auf die neuen/überarbeiteten regulatorischen Anforderungen hin anzupassen.

Ein weitere Herausforderung besteht darin, dass im Rahmen der Umsetzung und dann vor allem im weiteren Linienbetrieb die für regulatorische Themen zuständigen Stellen im Haus eingebunden werden müssen.

Auslagerungen sind somit beispielsweise (zukünftig) auch ein Thema des Risikomanagements, der Internen Revision, im Falle von IT-Auslagerungen auch des IT-Sicherheitsbeauftragten und im Falle von im Rahmen einer Auslagerung weitergegebenen personenbezogenen Daten auch des Datenschutzbeauftragten und Compliance ist i.d.R. auch immer dabei.

Hier gilt es, die Aufbauorganisation (Rollen und Verantwortlichkeiten) entsprechend weiterzuentwickeln und Wege für eine effiziente organisatorische und methodische Verzahnung der beteiligten Einheiten zu finden.

Haben Sie all diese Hürden gemeistert und ist Ihr Umsetzungsprojekt beendet oder steht kurz vor seinem Abschluss, dann sollten Sie einen prüfenden Blick auf die Arbeitsergebnisse werfen und sicherstellen, dass Sie nichts (wesentliches) vergessen haben.

Kommen wir nun zur Frage, wie Ihnen das vorliegende Arbeitsbuch bei der Erledigung dieser Aufgaben behilflich sein kann.

Das Arbeitsbuch EBA Leitlinien zu Auslagerungen stellt alle Anforderungen im Detail dar. Für eine schnelle Orientierung und eine optimale Bearbeitung haben wir eine Struktur entwickelt, die für jede Anforderung immer gleich ist. Sie besteht aus den folgenden Elementen:

- Norm-Bezug

  Hier wird die Textziffer genannt, unter der die jeweilige Anforderung im Originaltext zu finden ist.

  Den Norm-Bezug finden Sie auch als Spalte in der Checkliste.

- Thema

  Das Thema beschreibt den Inhalt der jeweiligen Anforderung in einem Satz oder Stichwort.

  Das Thema ist auch eine Spalte in der Checkliste.

- betroffene Funktion(en) / Einheit(en)

  Hier nennen wir Ihnen die aus unserer Sicht im Rahmen der Umsetzung miteinzubindenden Funktionen bzw. Organisationseinheiten.

  In der Checkliste können Sie bei Bedarf auch Ihre hausinternen Einheiten / Funktionen hinterlegen und zuordnen.

- Anforderung (Originaltext)

  Die eigentliche Anforderung führen wir hier im Originaltext auf. Bei europäischen Normen nehmen wir bis zur Veröffentlichung der offiziellen deutschen Übersetzung den englischen Originaltext.

- Öffnungsklausel(n) / Erleichterung(en)

  Öffnungsklauseln und sonstige Erleichterungen können dazu dienen, Ihren Umsetzungsaufwand erheblich zu reduzieren. Nehmen Sie diese Möglichkeiten in Anspruch ist es allerdings sehr wichtig, eine für Dritte nachvollziehbare Argumentation für die Inanspruchnahme zu formulieren. Ansonsten werden sich Prüfer mit dieser Umsetzung voraussichtlich nicht zufriedengeben.

- Handlungsoptionen / Umsetzungshinweise

  In diesem Abschnitt zeigen wir Ihnen die konkreten Handlungsoptionen auf und geben Ihnen Hinweise für eine effiziente Umsetzung.

  Wir müssen an dieser Stelle allerdings darauf hinweisen, dass es sich hier lediglich um Empfehlungen handelt, die wir nach bestem Wissen für Sie zusammengestellt haben.

  Eine Garantie, dass unsere Empfehlungen in jedem Fall prüfungsfest sind, können wir ausdrücklich nicht übernehmen.

  Dazu ist jedes Institut in seiner Aufbau- und Ablauforganisation (Größe/Komplexität) anders und auch die Prüfer haben immer wieder unterschiedliche Prüfungsschwerpunkte und Erwartungshaltungen, was die Anforderungsumsetzung betrifft.

Soweit der Theorie-Teil.

Nun geht es an die konkrete Umsetzung, den Praxis-Teil. Hierzu haben wir ebenfalls eine Struktur entwickelt, welche die wesentlichen Aspekte Ihrer Arbeit widerspiegelt und in Form eines Formulars für jede Anforderung zur Verfügung gestellt wird:

Tz. 18	**Proportionalität / Verhältnismäßigkeit der Anforderungsumsetzung in Bezug auf das betriebene Bankgeschäft (Fokus auf das Geschäft des Instituts)**
Beurteilung Relevanz:	
☐ JA ☐ NEIN	Begründung (wenn NEIN):
Beurteilung Handlungsbedarf:	
notwendige Umsetzungsaktivitäten:	

Was?	Wer?	Bis wann?

☐ Berücksichtigung in der sfO / im OHB
☐ Berücksichtigung im Kontrollumfeld / IKS
☐ Berücksichtigung bei Maßnahmen zum Datenschutz
☐ Berücksichtigung in der Prüfungsplanung IR

geplantes Umsetzungsdatum:	**geschätzter Umsetzungsaufwand:**

Notizen:

Abbildung 2: Vorlage zur Umsetzungsplanung

Textziffer und Titel haben wir aus dem Theorie-Teil übernommen.

Ab jetzt sind Sie an der Reihe.
Klären Sie zunächst die Relevanz der Anforderung für Ihr Institut. Sind Sie überhaupt betroffen? Wenn nicht, dann begründen Sie dies entsprechend. Eine nachvollziehbare Begründung ist in Prüfungssituationen Gold wert.

Beurteilen Sie dann den Handlungsbedarf. Besteht er überhaupt? Oder haben Sie die Anforderung bereits angemessen umgesetzt? Ist zum Beispiel eine Umsetzung auf Ebene des übergeordneten Instituts hinreichend, so dass Tochterinstitute in der Gruppe keine weiteren Umsetzungsarbeiten vornehmen müssen?

Wenn nein, dann ist es nun an der Zeit, sich Gedanken über die konkret notwendigen Umsetzungsaktivitäten zu machen. Was sollte wer bis wann erledigen?

Meistens zieht die Umsetzung einer regulatorischen Anforderung eine Reihe von zusätzlichen Aktivitäten nach sich (z.B. Dokumentation im Organisationshandbuch; Berücksichtigung im Internen Kontrollsystem; Auswirkungen auf den Schutz personenbezogener Daten; Ergänzung der Prüfungsplanung der Internen Revision). Stellen Sie fest, ob dies der Fall ist. Damit sind diese Aktivitäten Teil der Umsetzung und werden nicht vergessen.

In Abschnitt 4.7 Nachgelagerte Umsetzungsaktivitäten finden Sie weitere Informationen dazu.

Für Ihre Planung ist es i.d.R. von Vorteil, wenn eine erste Einschätzung des Fertigstellungsdatums vorliegt.

Gleiches gilt für den, mit der Umsetzung verbundenen, Arbeits- bzw. Ressourcenaufwand.

Fassen wir die Einsatzmöglichkeiten des vorliegenden Arbeitsbuchs noch einmal zusammen:

- Das Arbeitsbuch hilft Ihnen zunächst, auf der notwendigen Detailtiefe der Textziffern-Ebene, die einzelnen Anforderungen der Norm hinsichtlich Relevanz und Handlungsbedarf zu beurteilen.

- Dann unterstützt sie das Arbeitsbuch bei der Planung der konkreten Umsetzungsaktivitäten.

- Schließlich bietet Ihnen das Arbeitsbuch Reminder in Bezug auf nachgelagerte, aber i.d.R. immer notwendige weitere Umsetzungsaktivitäten, wie Dokumentation im Organisationshandbuch, Berücksichtigung im Internen Kontrollsystem oder im Datenschutzmanagement sowie in der Prüfungsplanung der Internen Revision.

- Für die Umsetzungsplanung wichtig sind häufig Angaben zu Fertigstellung sowie Arbeits- bzw. Ressourcenaufwand.

Mit Ihrem Arbeitsbuch haben Sie all diese Informationen (Theorie der Anforderung UND Praxis der Umsetzung) in der notwendigen Detailtiefe jederzeit griffbereit an einem Ort verfügbar und bei den mit Sicherheit notwendigen Meetings immer dabei.

Sollten Sie unabhängig von den auf Textziffern-Ebene dargestellten Anforderungen weitere Anforderungen selbst formulieren wollen, so stellen wir Ihnen unter 8.1 eine Druckvorlage zur Verfügung.

Gleiches gilt für das Umsetzungsformular. Sollten Sie mehr Platz benötigen oder für zusätzliche Anforderungen die Umsetzung planen wollen, dann nutzen Sie die entsprechende Druckvorlage unter 8.2.

Soweit unsere Hinweise zu den Einsatzmöglichkeiten unseres Arbeitsbuchs.

Im nächsten Abschnitt erfahren Sie, was es mit den ergänzenden Arbeitsmaterialien zum Arbeitsbuch auf sich hat.

3 Ergänzende Arbeitsmaterialien

Die Handlungsoptionen und Umsetzungshinweise geben Ihnen Hilfestellung für Ihr Umsetzungsprojekt.

Um die übersichtliche Darstellung der Anforderungen auf Textziffern-Ebene nicht zu gefährden und weil es in der Praxis häufig so ist, dass andere Einheiten eine konkrete Anforderung umsetzen müssen, haben wir uns dazu entschlossen, Ihnen weitere Umsetzungshilfen wie z.B. Inhaltsangaben (z.B. Mindestinhalte von Auslagerungsvereinbarungen) oder Schaubilder für ein besseres Verständnis, in separaten PDF-Dateien zur Verfügung zu stellen.

Zum Abschluss noch ein paar Worte zur Projekt- bzw. Zeitplanung Ihrer Umsetzungsarbeiten.

Die Projektplanung ist im Regelfall durch die regulatorischen Umsetzungsfristen maßgeblich geprägt. Bei den EBA Leitlinien zu Auslagerungen muss eine erste Umsetzung bis zum 30.09.2019 erfolgen.

Inwiefern die BaFin diese Umsetzungsfrist auch für Deutschland übernehmen wird, muss Sie im Rahmen des sogenannten Comply-or-Explain-Verfahrens gegenüber der EBA äußern.

Aktuell gehen wir davon aus, die Anforderungen der EBA Leitlinien zu Auslagerungen in die kommende MaRisk-Novelle übernommen werden. Diese zeichnet sich für das Jahr 2020 ab.

Sobald hierzu weitere belastbare Informationen vorliegen, werden wir Sie über unseren Newsletter darüber informieren.

Aber jetzt genug der Vorrede, mit dem nächsten Abschnitt starten wir mit Ihrem Umsetzungsprojekt.

4 Allgemeine Umsetzungshinweise

4.1 Normhintergrund / Normeinordnung

Wie jüngste Studien belegen, nimmt die Bedeutung von Auslagerungen im Bankensektor weiter zu. So planen 54% der befragten Institute in den kommenden ein bis zwei Jahren weitere Prozesse und Aktivitäten auszulagern[1].

Als Haupttreiber für diese Entwicklung werden von den Marktteilnehmern der weiter steigende Kostendruck sowie der direkte Zugriff auf die Expertise und das Fachwissen externer Dienstleister und FinTechs zur Weiterentwicklung des eigenen Geschäftsmodells, genannt.

Mit der Zunahme von Auslagerungen erhöht sich jedoch gleichzeitig die Abhängigkeit der Institute von ihren Service Providern. Fehler des Service Providers können zu Schäden für das auslagernde Institut führen.

Darüber hinaus finden Arbeitsabläufe und Geschäftsprozesse innerhalb von Auslagerungsbeziehungen über Unternehmensgrenzen hinweg statt. Dies erhöht die Komplexität und bietet Cyberkriminellen ein breiteres Spektrum an Möglichkeiten zu Cyberattacken.

Auch besteht die Gefahr, dass das Wissen um einmal ausgelagerte Aktivitäten im auslagernden Institut Stück für Stück verloren geht. Im Falle einer notwendigen Rückverlagerung verfügt das Institut nicht mehr über das benötigte Wissen.

Zu guter Letzt ist davon auszugehen, dass es durch den hohen Spezialisierungsgrad der Service Provider in u.U. kritischen Funktionsbereichen zu einer massiven Reduktion von Auswahlmöglichkeiten kommt. Der Bankensektor als Ganzes könnte dadurch in eine hohe Abhängigkeit von nur wenigen Service Providern geraten. Eine solche Entwicklung ist in Deutschland beispielsweise bei den Anbietern von Meldewesen-Software (Software as a Service) zu beobachten.

Die EBA trägt diesen Entwicklungen mit den neuen Leitlinien zu Auslagerungen nun Rechnung.

In der Folge werden die Leitlinien des Ausschusses der Europäischen Bankaufsichtsbehörden (CEBS) zum Outsourcing vom 14. Dezember 2006 aufgehoben.

Die bereits vorhandenen Empfehlungen der EBA zu Auslagerungen an Cloud-Anbieter werden in die neuen Leitlinien zu Auslagerungen überführt. Bisher hatte die BaFin unter Verweis auf die kommenden EBA Leitlinien wesentliche Aspekte dieser Empfehlungen noch nicht umgesetzt.

[1] Studie: Outsourcing in der Finanzindustrie – November 2018, PwC

Darüber hinaus verfolgt die EBA das Ziel, ein Rahmenwerk für Auslagerungen im Bankensektor zu schaffen, mit dem das EU-Recht und die damit verbundenen regulatorischen Anforderungen jederzeit gewahrt bleiben, insbesondere bei Geschäftsbeziehungen zu Service Providern mit Sitz in einem Nicht-EU-Staat (Drittland). Hierbei geht es insbesondere um den Schutz personenbezogener Daten, wenn diese im Rahmen von Auslagerungen außerhalb der EU verarbeitet werden.

Für deutsche Institute besteht die Herausforderung nun, die neuen Anforderungen der EBA mit den bereits bestehenden und umgesetzten Anforderungen der letzten MaRisk-Novelle sowie den bankaufsichtlichen Anforderungen an die IT (BAIT) in Einklang zu bringen.
Wir versuchen dieser Herausforderung im Weiteren Rechnung zu tragen, indem wir auf mögliche Abhängigkeiten zwischen den genannten Normtexten hinweisen.

4.2 Geltungsbereich

Auf EU-Ebene bilden die Eigenkapitalrichtlinie (Richtlinie 2012/36 - CRD), die Zahlungsdienstrichtlinie (Richtlinie 2015/2366 – PSD2) sowie die E-Geld-Richtlinie (2009/110/EG) die Rechtsgrundlage für die EBA Leitlinien zu Auslagerungen:

Damit fallen die folgenden Institute in den Geltungsbereich dieser Leitlinien:

- CRR-Institute (CRR-Kreditinstitute und CRR-Wertpapierfirmen)
- Zahlungsinstitute
- E-Geld-Institute

Die Vorgaben der Eigenkapitalrichtlinie, die die EBA mit den Leitlinien zu Auslagerungen nun konkretisiert, betreffen die interne Risikosteuerung der CRR-Institute und den Prozess ihrer Überprüfung und Bewertung (Supervisory Review and Evaluation Process – SREP) durch die Aufsicht.

Konkretere Vorgaben zu Auslagerungen für CRR-Institute, die bisher so nicht in der Bankenrichtlinie enthalten sind, werden im deutschen Aufsichtsrecht im § 25b KWG formuliert.

Grundsätzlich gelten die Vorgaben sowohl auf Einzelinstitutsebene als auch auf konsolidierter Ebene. Das EU-Recht sieht allerdings die Möglichkeit des so genannten „Waiver“ nicht nur für die Eigenkapitalanforderungen (sog. Säule I), sondern auch für Anforderungen an die Risikosteuerung (sog. Säule II) vor.

Sofern ein CRR-Institut einen diesbezüglichen „Säule-II-Waiver“ von der zuständigen Aufsichtsbehörde nach Durchlaufen des Antragsverfahrens erhalten hat, ist eine Umsetzung auf Einzelinstitutsebene nicht notwendig.

Ansonsten führt an einer Umsetzung der Anforderungen kein Weg vorbei.

Nach Tz. 10 der EBA Leitlinien zu Auslagerungen sollen Zahlungsinstitute und E-Geld-Institute den Vorgaben auf Einzelinstitutsebene nachkommen.

Generell ist somit davon auszugehen, dass jedes Institut auf Einzelebene eine Umsetzung der EBA Leitlinien zu Auslagerungen vornehmen muss. Auf die Öffnungsklauseln zur Umsetzung auf Gruppenebene bzw. im Institutsverbund gehen wir im Folgenden bei unserem Umsetzungsempfehlungen zu den jeweiligen Detailanforderungen in den einzelnen Textziffern ein.

4.3 Aufbau und Themenschwerpunkte der Norm

Die Leitlinien zu Auslagerungen gliedern sich aus Institutssicht in vier Titel.

Der fünfte Titel beschreibt die Anforderungen, welche die EBA an die nationalen Aufsichtsbehörden im Zusammengang mit Auslagerungen stellt. Darin enthalten sind Vorgaben zu den Überprüfungshandlungen der zuständigen Aufsichtsbehörden in Rahmen des SREP.

Wir haben Titel V (noch) nicht behandelt, da gegenwärtig noch nicht absehbar ist, wie die EZB-Bankenaufsicht sowie BaFin und Bundesbank mit diesen Anforderungen umgehen werden.

Über die weiteren Entwicklungen in diesem Themenkomplex werden wir Sie in unserer vierteljährlich erscheinende Regulatorischen Agenda informieren.

Nachfolgend nun ein kurzer Überblick über die vier, für Institute relevante, Titel. Die jeweiligen Textziffern werden im Detail in Abschnitt 5 Anforderungen im Detail dargestellt.

Titel I: **Prinzip der Verhältnismäßigkeit und Umsetzung der Anforderungen innerhalb von Institutsgruppen sowie in Instituten, die Mitglieder eines institutsbezogenen Sicherungssystems sind (Tz. 18-25)**

Die betroffenen Institute sollten sich bei der Ausgestaltung ihres Auslagerungsmanagements am **Prinzip der Verhältnismäßigkeit** (Proportionalitätsprinzip) orientieren.

Auf welche Bezugsgrößen die EBA dabei abstellt, findet sich in Abschnitt 1.

Abschnitt 2 gibt Auskunft darüber, welche Aspekte des Auslagerungsmanagements die EBA bei **Auslagerungen innerhalb von Institutsgruppen sowie bei Instituten, die Mitglieder eines institutsbezogenen Sicherungssystems sind**, für besonders wichtig erachtet.

So verbleibt beispielsweise die **Verantwortung für die ausgelagerten Tätigkeiten** bei Auslagerungen innerhalb einer Institutsgruppen immer bei der Geschäftsleitung des jeweils auslagernden Instituts.

Sofern für die gesamte Institutsgruppe ein **zentrales Auslagerungsregister** geführt wird, muss sichergestellt sein, dass jederzeit für jedes Institut der Gruppe ein Register auf Einzelinstitutsebene erstellt werden kann.

Erfolgt eine **zentrale Überwachung der Auslagerungen**, sollte jedes gruppenangehörige Institut regelmäßig und bei Bedarf anlassbezogen Berichte über den Überwachungsstatus erhalten.

Bei einer **zentrale**n **Vorabbeurteilung der Auslagerung** muss sichergestellt sein, dass die jeweils spezifische Risikosituation der einzelnen Gruppeninstitute angemessen berücksichtigt wird.

Kommt ein **zentraler Gruppenausstiegsplan** zum Einsatz, so sind auch hier die Spezifika der einzelnen Gruppeninstitute angemessen zu berücksichtigen.

Titel II: Grundsätze zur Beurteilung von Auslagerungsvereinbarungen (Tz. 26-31)

Zunächst müssen Institute prüfen, ob eine Vereinbarung mit einem Dritten unter die **Definition** des Begriffs **Auslagerung** fällt.

Dabei ist es hilfreich, dass die EBA auch eine **Negativdefinition** formuliert, was explizit **keine Auslagerung** darstellt.

Des Weiteren definiert die EBA den **Gegenstand einer Auslagerung**.

Aus EBA-Sicht werden immer **Funktionen** ausgelagert.

Bei einer Funktion kann es sich um einen **Geschäftsprozess**, einen **Arbeitsablauf** bzw. eine **Geschäftsaktivität/-tätigkeit** oder eine **Dienstleistung** handeln.

Jede Funktion ist hinsichtlich ihrer **Kritikalität** (kritisch/nicht kritisch) bzw. **Bedeutung** (wesentlich/nicht wesentlich) zu beurteilen und entsprechend zu kategorisieren.

Zur Einschätzung von Kritikalität bzw. Bedeutung schlägt die EBA eine Reihe von **Bewertungskriterien** vor.

Wird eine **kritische/wesentliche Funktion** ausgelagert, so spricht die EBA in der Folge von einer **kritische**n**/wesentliche**n **Auslagerung**.

Für Institute, die unter die Regulierung der MaRisk bzw. BAIT fallen, stellt sich hier die Frage,

ob unter einer kritischen/wesentlichen Auslagerung nach den EBA Leitlinien das Gleiche zu verstehen ist, wie unter einer wesentlichen Auslagerung nach AT 9 Tz. 2 der geltenden MaRisk vom 27.10.2017.

Aus unserer Sicht ist an dieser Stelle ein Blick in das Merkblatt „Orientierungshilfe zu Auslagerungen an Cloud-Anbieter“ der BaFin vom November 2018 hilfreich.

Dort schreibt die Aufsichtsbehörde auf Seite 4:
„Im Folgenden wird der Begriff „**wesentlich**“ für die Begrifflichkeiten „wichtig/kritisch“ im Sinne des Artikels 274 Delegierte Verordnung(EU) 2015/35 und des § 32 VAG verwendet sowie für den Begriff „wesentlich“ im Sinne des § 25b KWG und § 26 ZAG.“

Kritische/wichtige Auslagerungen gemäß EBA Leitlinien stellen somit **wesentliche Auslagerungen** gemäß MaRisk bzw. BAIT dar.

Dies bedeutet, dass somit bei der Wesentlichkeitseinstufung gemäß AT 9 Tz. 2 MaRisk auch die Vorgaben der EBA Leitlinien zur Definition kritischer oder wesentlicher Funktionen (Tz. 29-31) berücksichtigt werden müssen.

Titel III: Steuerungsrahmen für Auslagerungen

In Titel III legt die EBA ihre Anforderungen an die Institute in Bezug auf die **Steuerung von Auslagerungen** ausführlich dar.

Sie betont, dass die **Verantwortung für die Erfüllung regulatorischer Anforderungen** (insbesondere der jederzeitigen Erfüllung der Bedingungen der Erlaubnisanforderungen zum Betreiben von Bankgeschäften) weiterhin beim auslagernden Institut verbleibt.

Die **Geschäftsleitung** des Instituts hat dieser Verantwortung durch die Wahrnehmung einer ganzen **Reihe von Aufgaben** Rechnung zu tragen.

Zentrales Element ist ein **ganzheitliches Risikomanagement**, welches das auslagernde Institut zu betreiben hat.

Zu den zu betrachtenden Risiken zählen auch das sogenannte **Risiko durch Dritte** (**Third-Party-Risk**), also **das Risiko, die sich aus Vertragsbeziehungen mit Dritten ergeben** kann.

Nach unserer Lesart ist es **zukünftig für ein ganzheitliches Risikomanagement grundsätzlich unerheblich**, **ob** es sich bei dieser Vertragsbeziehung um eine **Auslagerung** (z.B. Zahlungsabwicklung durch einen Dienstleister) **oder** um einen **Fremdbezug** (Kauf einer Software zum Reisemanagement mit anschließendem internen Betrieb) handelt.

Institute müssen diese Risikoart im Sinne des geforderten ganzheitlichen Risikomanagements

entsprechend berücksichtigen.

Somit ist mit Inkrafttreten der EBA Leitlinien zu Auslagerungen **jede Auslagerung sowie jeder Fremdbezug** (abweichend von den Anforderungen der BAIT, die sich nur auf IT-Fremdbezüge beziehen), **risikotechnisch** zu **betrachten**.

Wir gehen davon aus, dass das **Third-Party-Risk Management**, d.h. die Erfassung und Beurteilung sowie fortlaufende Überprüfung aller betroffenen Vertragsbeziehungen einen nicht unerheblichen Arbeitsaufwand in den Instituten verursachen wird.

Darüber hinaus sind vor allem bei kritischen/wesentlichen Auslagerungen alle (**operationellen**) **Risiken** einer ausgelagerten Funktion weiterhin so zu betrachten, als wäre die Funktion nicht ausgelagert.

Gleiches gilt für **Risiken bzgl.** der **IT-Sicherheit** sowie des **Datenschutzes**.

Im Endergebnis erweitern Auslagerungen und der Fremdbezug zukünftig das Aufgabenspektrum des internen Risikomanagements/Risikocontrollings beträchtlich.

Neben dem Risikomanagement von Auslagerungen fordert die EBA auch die fortlaufende **Überwachung von** insbesondere **kritischen/wesentlichen Auslagerungen**.

Teil des geforderten Steuerungsrahmens ist ebenfalls eine **Auslagerungsrichtlinie**, für welche die EBA gewisse Mindestinhalte definiert.

Das auslagernde Institut hat mögliche **Interessenkonflikte**, die mit einer Auslagerung einhergehen können, zu identifizieren, zu bewerten und zu lösen.

Zur Aufrechterhaltung des Geschäftsbetriebs (**Business Continuity Management**) hat das auslagernde Institut angemessene Maßnahmen auch für ausgelagerte Funktionen zu ergreifen bzw. sicherzustellen, dass der Service Provider dies entsprechend tätigt.

Die **Interne Revision** des auslagernden Instituts sollte in der Lage sein, eine unabhängige **Prüfung von Auslagerungen** durchführen zu können. Die von der EBA dazu festgelegten **Mindestinhalte** sind von der Internen Revision in ihrer **Prüfungsplanung** zu berücksichtigen.

Institute müssen ein **Verzeichnis aller Auslagerungsvereinbarungen** führen. Sie müssen in der Lage sein, den zuständigen Aufsichtsbehörden **auf Anfrage** dieses **Auslagerungsregister** zur Verfügung zu stellen.

Das im Entwurf der Leitlinien geplante **regelmäßige Reporting an die Aufsicht** sowie das dazu zur Verfügung gestellte **Template im Microsoft Excel-Format** wurden **nicht** in **die finale Fassung übernommen**. Das Reporting-Template ist allerdings weiterhin als Excel-Anlage zum

sog. final Report auf der Internetseite der EBA in englischer Sprache veröffentlicht.

Titel IV: Auslagerungsprozess (Tz. 61-108)

In Titel IV beschreibt die EBA die, aus ihrer Sicht, zentralen Arbeitsschritte, die ein Institut auf dem Weg zu einer Auslagerung durchlaufen sollte.

Zur besseren Verdeutlichung haben wir aus den EBA-Vorgaben das nachfolgende **Phasen-Modell** abgeleitet:

Abbildung 3: Phasen einer Auslagerung

In der **Vorvertragsphase** geht es darum, zunächst die Rahmenbedingungen für ein mögliches Auslagerungsvorhaben abzuklären. Dazu fordert die EBA von den Instituten Folgendes:

- Prüfung, ob die **aufsichtsrechtlichen Bedingungen für eine Auslagerung** erfüllt sind
- Beurteilung der **Auswirkungen** einer Auslagerung **auf das operationelle Risiko** des Instituts – wir empfehlen hier die direkte Erweiterung um eine Beurteilung von Reputationsrisiken, Risiken für den Datenschutz und die IT-Sicherheit sowie möglicher Risikokonzentrationen in Bezug auf die genannten Risiken
- **Due Diligence** der in Frage kommenden **Service Provider** (Beurteilung des Adressenausfallrisikos sowie ggf. des damit verbundenen Stützungsrisikos – Step-in-Risk)

In der **Vertragsphase** dreht sich dann alles um die Ausgestaltung der Auslagerungsvereinbarung.

Die EBA gibt hier bestimmte **Mindestinhalte** vor, die sich in den Vereinbarungen wiederfinden müssen.

Sofern das Institut einer **Weiterverlagerung** (Sub-Auslagerung) zustimmt, sollten Auslagerungsvereinbarungen weitergehende Aspekte beinhalten.

Zentrale Themen sollten auf jeden Fall vertraglich geregelt sein. Dazu zählen u.a.:

- Regelungen zur **Sicherheit von Systemen und Daten**

- explizite **Auskunfts-, Zugangs- und Prüfungsrechte** für die Interne Revision des auslagernden Instituts sowie die zuständigen Aufsichtsbehörden

- explizites **Kündigungsrecht**

Während der anschließenden **Betriebsphase** fordert die EBA von einem auslagernden Institut eine angemessene **Auslagerungsüberwachung**. Dies gilt sowohl in Bezug auf die **Qualität der Leistungserbringung**, als auch in Bezug auf die **Vitalität des Service Providers**.

Im Falle der planmäßigen oder außerplanmäßigen Beendigung einer Auslagerung, tritt das auslagernde Institut in die **Beendigungs-/Rückverlagerungsphase** ein.

Das auslagernde Institut sollten sicherstellen, dass **Auslagerungsvereinbarungen ohne unzumutbare Unterbrechung ihrer Geschäftstätigkeiten** oder **negativer Auswirkungen auf die Einhaltung der aufsichtlichen Anforderungen** und die **Kontinuität und Qualität der Dienstleistungen gegenüber ihren Kunden** beendet werden können.

Dazu hat es eine entsprechende **Ausstiegsstrategie** für jede Auslagerung zu entwickeln und regelmäßig auf ihre Umsetzbarkeit hin zu überprüfen (**Ausstiegsplan**).

Obwohl sich **Titel V** an die nationalen Aufsichtsbehörden richtet, möchten wir zum Schluss noch auf einen, aus Sicht der Institute, wahrscheinlich begrüßenswerten Aspekt hinweisen.

In der finalen Fassung ihrer Leitlinien zu Auslagerungen hat die EBA **auf** die **Dokumentationsvorlage für Auslagerungen verzichtet**. Auch die zunächst angekündigte **Meldepflicht** findet sich gegenwärtig **nicht mehr**.

Allerdings müssen **auslagernde Institute** in der Lage sein, die nationalen Aufsichtsbehörden **auf Anfrage mit allen gewünschten Informationen** zu **versorgen**.

Dazu zählen:

- das Auslagerungsregister

- die (auch gemäß MaRisk; BAIT) über die Laufzeit fortzuschreibende Risikoanalyse für jede Auslagerung

- eine Dokumentation über die Wirksamkeit der Leistungsüberwachung des auslagernden Instituts über den Service Provider

- eine Ausstiegstrategie des auslagernden Instituts

Bei der Konzeption des Auslagerungsregisters empfiehlt es sich daher, sich an dem in MS-Excel vorliegenden Muster zu orientieren.

Soweit unser Überblick über den Aufbau sowie die wesentlichen Inhalte der EBA Leitlinien zu Auslagerungen.

Das nachfolgende Schaubild stellt die Struktur bzw. den Aufbau der EBA Leitlinien zu Auslagerungen noch einmal visuell dar.

Title I – Proportionality: group application and institutional protection schemes
Titel I – Verhältnismäßigkeit: gruppenweite Anwendung und institutsbezogene Sicherungssysteme

1 Verhältnismäßigkeit
2 Auslagerung durch Gruppen und Institute, die Mitglieder eines institutsbezogenen Sicherungssystems sind

Title II – Assessment of outsourcing arrangements
Titel II – Bewertung von Auslagerungsvereinbarungen

3 Auslagerung
4 Kritische oder wesentliche Funktionen

Title III – Governance framework
Titel III – Rahmen für die Governance

5 Solide Governance-Regelungen und Risiko durch Dritte („Third-Party Risk")
6 Solide Governance-Regelungen und Auslagerungen
7 Auslagerungsrichtlinien
8 Interessenkonflikte
9 Geschäftsfortführungspläne
10 Funktion der Internen Revision
11 Dokumentationsanforderungen

Title IV – Outsourcing process
Titel IV – Auslagerungsprozess

12 Analyse vor der Auslagerung
13 Vertragsphase
14 Beaufsichtigung der ausgelagerten Funktionen
15 Ausstiegsstrategien

Title V – Guidelines on outsourcing addressed to competent authorities
Titel V – An die zuständigen Behörden gerichtete Leitlinien zu Auslagerungen

Abbildung 4:Struktur/Aufbau der EBA Leitlinien zu Auslagerungen

4.4 Betroffene Funktionen

In diesem Abschnitt unseres Arbeitsbuchs möchten wir Ihnen einen Überblick über die, aus unserer Sicht, von der Umsetzung der EBA Leitlinien betroffenen Funktionen bzw. Einheiten in Ihrem Institut geben.

Wir verwenden die Begriffe Funktion und (Organisations-)Einheit synonym und meinen damit alle Stellen im Haus, die sich mit der Auslagerungsthematik befassen (müssen).

Da es sich bei Auslagerungen um komplexe Vorhaben handelt, beanspruchen sie in der Regel in vielfältiger Weise die Fach-Expertise und die Management-Skills unterschiedlicher Funktionen.

Ein wichtiger Erfolgsfaktor für das Gelingen Ihres Umsetzungsprojektes besteht somit in der Koordination dieser verschiedenen Funktionen.

Ob zunächst als Verantwortliche/r für das Umsetzungsprojekt oder später als zentrale/r Auslagerungsverantwortliche/r, beziehen Sie die anderen betroffenen Funktionen beizeiten mit ein, kombinieren Sie das Vorhandene mit dem Neuen und kommunizieren Sie fortlaufend über Ziele, Status, Herausforderungen bei der Umsetzung und vor allem die Umsetzungserfolge.

Beteiligungsmanagement

Ist das auslagernde Institut direkt oder indirekt (z.B. über eine Beteiligungsholding) am Service Provider (Auslagerungsunternehmen gemäß des MaRisk) beteiligt, an den eine Funktion ausgelagert ist bzw. werden soll, so sollten Sie auch das interne Beteiligungsmanagement in das Umsetzungsprojekt miteinbeziehen.

Über das Beteiligungsmanagement erhalten Sie Auskunft über Ausgestaltung und Umfang der Beteiligung. Diese Aspekte können einen bedeutende Rolle bei der Risikoanalyse des Service Providers spielen (insbesondere Step-in Risk/Stützungsrisiko).

Ggf. kann es sinnvoll oder sogar notwendig sein, das Beteiligungsmanagement bei der Überwachung der ausgelagerten Funktionen miteinzubeziehen. Dies könnte bereits zur Erfüllung der Anforderungen aus AT 9 Tz. 9 MaRisk erfolgen.

Meldewesen/Regulatory Office

Das Meldewesen stellt i.d.R. die Informationsschnittstelle zur Aufsichtsbehörde dar. Die zuständigen Aufsichtsbehörden, d.h. EZB-Bankenaufsicht und BaFin/Bundesbank sind nach den EBA Leitlinien gehalten, sich durch den Abruf von Teilen oder des ganzen

Auslagerungsregisters ein Bild über den Umfang und die Ausgestaltung der Auslagerungen in den Instituten zu machen.

In welcher Weise solche Abfragen erfolgen, müssen die Aufsichtsbehörden noch festlegen. Grundsätzlich sind hier eine regelmäßige Zumeldung über die üblichen Meldewesenschnittstellen, eine Abfrage im Rahmen des jährlichen SREP oder gesonderte Zulieferungsanfragen denkbar.

Im letzteren Fall ist i.d.R. das so genannte „Regulatory Office“ des Instituts zuständig, d.h. diejenige Stelle, welche die Anfragen der Aufsicht an die Geschäftsleitung bündelt.

Institute unter direkter EZB Aufsicht (so genannte bedeutende Institute – Significant Institutions) müssen seit einiger Zeit im Rahmen des SREP jährlich ein so genanntes SREP-Paket, d.h. eine umfangreiche Zusammenstellung bankinterner Unterlagen zur Risikosteuerung zusammen mit dem ICAAP-Statement und dem ILAAP-Statement der Geschäftsleitung liefern. Es ist anzunehmen, dass das mit den EBA Leitlinien geforderte Auslagerungsregister von der EZB als Teil dieses Pakets im Rahmen des SREP zukünftig geprüft werden wird.

Informieren Sie das Meldewesen und das Regulatory Office über diese regulatorische Neuerung und legen Sie fest, wer für die Bearbeitung einer solchen Anfrage durch die Aufsichtsbehörde zuständig ist und wie die Bearbeitung ablauforganisatorisch erfolgt.

Geschäftsleitung

Die EBA Leitlinien heben besonders die ausdrücklich Verantwortung der Geschäftsleitung des auslagernden Instituts hervor.

Im Rahmen einer Auslagerung hat die Geschäftsleitung u.a. die folgenden Aufgaben wahrzunehmen:

- Sie muss sicherstellen, dass zu jederzeit die Bedingungen für die Erteilung der Geschäftserlaubnisse erfüllt sind.
- Sie muss alle Auslagerungen unter Risikoaspekten fortlaufend betrachten.
- Sie muss die Qualität der Leistungserbringung fortlaufend überwachen.
- Sie muss Interessenkonflikte aktiv managen.
- Sie muss zumindest bei kritischen/wesentlichen Auslagerungen sicherstellen, dass das Institut angemessene Maßnahmen zur Aufrechterhaltung des Geschäftsbetriebs

ergriffen hat sowie über eine wirksame Ausstiegsstrategie zur Rückverlagerung bzw. zum Wechsel des Service Providers verfügt.

Die Geschäftsleitung sollte in diesem Umsetzungsprojekt ein zentraler Stakeholder sein.

Auslagerungsverantwortliche

Die/der Auslagerungsverantwortliche ist nach unserem Verständnis die zentrale Person im Rahmen des Umsetzungsprojektes. Ggf. ist dieser fachliche Themenverantwortliche bereits der Auslagerungsbeauftragte des Instituts oder wird es nach Abschluss des Projekts.

Gemäß AT 9 Tz. 12 MaRisk haben die Institute in Abhängigkeit von Art, Umfang und Komplexität der Auslagerungsaktivitäten ein zentrales Auslagerungsmanagement einzurichten. Sofern eine solche Einheit im Institut besteht, verstehen wir den Auslagerungsverantwortlichen als den fachlichen Leiter dieser Funktions- bzw. Organisationseinheit.

Das eTraining der MARISK ACADEMY und damit auch dieses Arbeitsbuch richtet sich in erster Linie an den Auslagerungsverantwortlichen und soll ihn bei der Umsetzung seines Projektes unterstützen.

Risikomanagement / Risikocontrolling

Zentraler Dreh- und Angelpunkt der EBA Leitlinien ist die Einschätzung des mit der Auslagerung verbundenen Risikos (Auslagerungsrisiko) für das auslagernde Institut.

Dem Risikomanagement bzw. Risikocontrolling kommt somit eine zentrale Bedeutung im Rahmen des Auslagerungsmanagements zu.

Nach unserem Verständnis können diese Aufgaben des Risikomanagements vom zentralen Auslagerungsmanagement wahrgenommen werden, sofern dieses operativ in der so genannten 2nd Line of defence, d.h. der zweiten Verteidigungslinie angesiedelt ist.

Gemäß AT 9 Tz. 12 sind die Risikoanalysen in der 1st Line of defence, d.h. von den für die Auslagerung primär zuständigen Bereichen durchzuführen. Dem zentralen Auslagerungsmanagement kommt dabei allerdings die Funktion der Koordination und Überprüfung der Risikoanalysen zu.

Rechtsabteilung

Auslagerungen sind komplexe Vorhaben, die einer detaillierten vertraglichen Vereinbarung zwischen auslagerndem Institut und Service Provider bedürfen.

Informieren Sie Ihre Rechtsabteilung umfassend über die regulatorischen Anforderungen an Auslagerungsvereinbarungen (insbes. Mindestinhalte).

Stellen Sie sicher, dass auch alle bestehenden Vereinbarungen in Bezug auf die „neuen" Mindestinhalte geprüft und ggf. angepasst werden. Beachten Sie dabei die festgelegten Umsetzungsfristen bzw. Übergangsregelungen.

Compliance

Die Compliance-Funktion hat gemäß 4.4.2 MaRisk auf die Beachtung aller relevanten (internen und externen) Regelungen im Institut hinzuwirken (Regelkonformität).

Aufgrund ihres bereits dargestellten Geltungsbereichs umfasst dies auch die vorliegenden EBA Leitlinien zu Auslagerungen.

Besonderes Augenmerk sollte die Compliance-Funktion während des Umsetzungsprojekts auf folgende Aspekte legen:

- Unabhängige Beurteilung der Verhältnismäßigkeit der Umsetzung unter Berücksichtigung der Kriterien zur Verhältnismäßigkeit gemäß I.1 Tz. 18/19.

- Unabhängige Beurteilung der Umsetzung im Hinblick auf die bestehende interne Governance sowie die Anforderungen gemäß I.1 Tz. 20.

IT-Sicherheitsbeauftragter

Sind von einer Auslagerung IT-Systeme bzw. Prozesse betroffen, die von IT-Systemen unterstützt werden, so spielt die Sicherheit dieser Systeme bzw. der dort verarbeiteten Daten eine wichtige Rolle.

In diesen Fällen ist der IT-Sicherheitsbeauftragte des auslagernden Instituts in das Umsetzungsprojekt einzubinden.

Wenn es um die Frage geht, wie gut es um die IT-Sicherheit des Service Providers bestellt ist, muss/sollte der IT-Sicherheitsbeauftragte des auslagernden Instituts seine Expertise einbringen.

Datenschutzbeauftragter

Werden im Rahmen einer Auslagerung personenbezogene Daten verarbeitet, so ist der Datenschutzbeauftragte des auslagernden Instituts einzubeziehen.

Interne Revision

Gemäß 4.4.3 Tz. 3 MaRisk hat die Interne Revision die Angemessenheit des Risikomanagements und des Internen Kontrollsystems sowie die Ordnungsmäßigkeit aller Aktivitäten und Prozesse sowie IT-Systeme zu überprüfen.

Auslagerungen bilden hier keine Ausnahme. Im Gegenteil. Wie die EBA Leitlinien durch ihre Forderung nach weitgehenden Informations- und Prüfungsrechten an die Service Provider unterstreicht, kommt der Internen Revision des auslagernden Instituts eine zentrale Rolle bei der Überprüfung einer Auslagerung zu.

Informieren Sie die Interne Revision Ihres Hauses umfassend über ihre Pflichten und Rechte mit Bezug auf die Auslagerungsthematik.

Stellen Sie sicher, dass die Prüfungsplanung der Internen Revision das Thema angemessen berücksichtigt.

Insbesondere die folgenden Aspekte sollten durch die Interne Revision beachtet werden:

- Prüfung der Auslagerungsrichtlinie
- Prüfung des Risikomanagements in Bezug auf Auslagerungen
- Prüfung des Vorgehens zur Leistungsüberwachung
- Prüfung des Auslagerungsmanagements im Allgemeinen
- Prüfung Datenschutzmaßnahmen im Rahmen der Auslagerung;

Wirtschaftsprüfer / weitere externe Prüfer/Auditoren

Einige Vorgaben der EBA Leitlinien beziehen sich auf die Rolle der Wirtschaftsprüfer (vgl. z.B. Tz. 87). Darüber hinaus können im Institut weitere externe Prüfer tätig sein, z.B. unterstützend zur Revision oder bankinternen Validierungseinheit.

Soweit Sie von der Möglichkeit, einen externen Auditor einzusetzen, Gebrauch machen können bzw. wollen, sollten Sie sich über dessen Fachexpertise ein angemessenes Bild machen (z.B. Reverenzen, Zertifikate u.ä.) und dies auch dokumentieren.

Bei der Tätigkeit des Wirtschaftsprüfers sind die Vorgaben der Prüfungsberichtsverordnung

(PrüfbV – Verordnung über die Prüfung der Jahresabschlüsse der Kreditinstitute und Finanzdienstleistungsinstitute sowie über die darüber zu erstellenden Berichte) zu beachten.

Interne IT

Da Auslagerungen fast immer IT-Systeme betreffen, ist die interne IT ebenfalls in das Umsetzungsprojekt einzubinden.

Aus Sicht der Leitlinien sollte die interne IT vor allem bei den folgenden beiden Punkten mitwirken:

- Penetrationstests zur Bewertung von Cyber- und ITK-Risiken gemäß IV.13.3 Tz. 94
- Auswahl geeigneter Prüfer bei Prüfungen mit hoher IT-technischer Komplexität gemäß IV.13.3 Tz. 97

Einkauf / Beschaffung

Die EBA Leitlinien fordern ein umfassendes Risikomanagement. Gemäß III.5 Tz. 32/33/34 gilt dies nicht nur für Auslagerungen, sondern ebenso auch für alle sonstige Vereinbarungen mit Dritten (sog. Risiko durch Dritte/Third Party Risk).

Damit sind auch alle anderen Einkäufe, Anschaffungen, Beschaffungsvorgänge, also alles was man unter sonstigem Fremdbezug subsumieren kann, einer Risikoanalyse zu unterziehen.

Allerdings halten wir es in diesem Zusammenhang für vertretbar, wenn sonstige Fremdbezüge zu Gruppen mit gleichen/ähnlichen Charakteristika zusammengefasst werden und eine Risikoanalyse auf „Gruppenebene“ erfolgt.

Auch eine „Gruppierung“ nach Hersteller bzw. Lieferanten würden wir als angemessen erachten.

Binden Sie deshalb auch Ihren Einkauf bzw. Ihre Beschaffung mit ein.

Business Continuity Management

Der störungsfreie Geschäftsbetrieb muss auch im Falle von Auslagerungen durch wirksame Maßnahmen sichergestellt werden.

Somit ist auch das Business Continuity Management (BCM) des auslagernden Instituts Teil des

Umsetzungsprojekts. Unter dem BCM verstehen wir die zuständige Einheit für die Umsetzung der Anforderungen zum Notfallkonzept aus AT 7.2 MaRisk.

Einheiten, in denen ausgelagert wird/wurde

Bei der Umsetzung dieser EBA Leitlinien sollten Sie auch die dezentralen Auslagerungsverantwortlichen, welche die Schnittstelle zwischen der internen Einheit und dem Service Provider bilden, umfassend einbeziehen.

Vermitteln Sie diesen Mitarbeitern das notwendige Wissen, um auch auf operativer Ebene die Einhaltung der hier formulierten regulatorischen Anforderungen sicherzustellen.

4.5 Umsetzungsfrist(en) & Übergangsregelung(en)

Mit Ausnahme von Tz. 63 (b) gelten diese Leitlinien ab dem 30. September 2019 für alle Auslagerungsvereinbarungen, die ab diesem Zeitpunkt abgeschlossen, überprüft und ggf. geändert werden.

Tz. 63 (b) erlaubt eine Auslagerung von Bankgeschäften oder Zahlungsdiensten an einen Service Provider mit Sitz in einem Drittstaat nur dann, wenn zwischen den für die Beaufsichtigung des auslagernden Instituts zuständigen Aufsichtsbehörden und den für die Beaufsichtigung des Dienstleisters zuständigen Behörden eine geeignete Kooperationsvereinbarung besteht.

Für diese Anforderung gilt eine Umsetzungsfrist bis zum 31. Dezember 2021. Hierzu ist insbesondere auch die weitere Entwicklung zum Brexit zu beachten, wodurch Großbritannien voraussichtlich zu einem Drittstaat werden wird, mit dem die deutschen Aufsichtsbehörden bzw. die EZB-Bankenaufsicht entsprechende Kooperationsvereinbarungen schließen müssen.

Vor dem genannten Hintergrund besteht eine zentrale Aufgabe in Ihrem Umsetzungsprojekt in der Überprüfung aller bestehenden Auslagerungsvereinbarungen.

Ist die Überprüfung von als kritisch/wesentlich einzustufenden Auslagerungen nicht bis zum 31. Dezember 2021 abgeschlossen, so fordert die EBA die Institute auf, ihre zuständige Aufsichtsbehörde darüber zu informieren.

Ebenso ist die Aufsichtsbehörde über die geplanten Maßnahmen zum Abschluss der Überprüfung oder der möglichen Ausstiegsstrategie zu unterrichten.

Institute sollten die Dokumentation aller bestehenden Auslagerungsvereinbarungen, mit Ausnahme von solchen mit einem Cloud Service Provider, im Einklang mit diesen Leitlinien nach dem ersten Verlängerungsdatum jeder bestehenden Vereinbarung, spätestens jedoch bis zum 31. Dezember 2021, vervollständigen.

Bestehende Vereinbarungen mit Cloud Service Providern sollten bereits schon jetzt entsprechend dokumentiert sein.

4.6 Definitionen

Die EBA Leitlinien arbeiten mit einer ganzen Reihe von Begriffen, welche sie vorab definiert. Dies erfolgt in Tz. 12 der EBA Leitlinien zu Auslagerungen. Bitte beachten Sie, dass auch die mittlerweile mit der deutschen Version der Leitlinien vorliegenden amtlichen Übersetzungen dieser Begriffe nicht zu den in den deutschen Rechtstexten gebräuchlichen Rechtsbegriffen konsistent sind.

Wir geben diese Begriffsdefinitionen im Folgenden wieder und ergänzen Sie in Teilen, insbesondere im Hinblick auf eine Abgrenzung zu den im deutschen Kontext gebräuchlichen Definitionen der MaRisk sowie der BAIT.

Begriff	**Definition**
Auslagerung	bezeichnet eine Vereinbarung in irgendeiner Form zwischen einem Institut, einem Zahlungsinstitut oder einem E-Geld-Institut und einem Dienstleister, mit der dieser Dienstleister einen Prozess, eine Dienstleistung oder eine Tätigkeit ausführt, die ansonsten von dem Institut, dem Zahlungsinstitut oder dem E-Geld-Institut selbst durchgeführt würde
Funktion	bezeichnet alle Prozesse, Dienstleistungen oder Aktivitäten
kritische oder wesentliche Funktion	bezeichnet jede Funktion, die als kritisch oder wesentlich im Sinne von Abschnitt 4 dieser Leitlinien angesehen wird
Weiterverlagerung	bezeichnet eine Situation, in der der Dienstleister im Rahmen einer Auslagerungsvereinbarung eine ausgelagerte Funktion weiter auf einen anderen Dienstleister überträgt.
Dienstleister	bezeichnet ein Drittunternehmen, das im Rahmen einer Auslagerungsvereinbarung einen ausgelagerten Prozess, eine ausgelagerte Dienstleistung oder Tätigkeit oder Teile davon durchführt. Die MaRisk sprechen in diesem Zusammenhang von Auslagerungsunternehmen (siehe AT 9 MaRisk).
Cloud-Dienst	bezeichnet Dienste, die unter Verwendung von Cloud Computing bereitgestellt werden, d.h. ein Modell für den allgegenwärtigen, bequemen On-Demand-Netzwerkzugriff auf einen gemeinsamen Pool von konfigurierbaren Computerressourcen (z.B. Netzwerke, Server, Speicher, Anwendungen und Dienste), die mit minimalem Verwaltungsaufwand oder Dienstanbieterinteraktion schnell bereitgestellt und freigegeben werden können.

	Die BAIT sprechen hier von Cloud-Dienstleitungen (siehe Abschnitt 8 Tz. 52)
Öffentliche Cloud	bedeutet Cloud-Infrastruktur, die der Allgemeinheit offen zur Verfügung steht.
Private Cloud	bedeutet Cloud-Infrastruktur, die ausschließlich für die Nutzung durch ein einzelnes Institut oder Zahlungsinstitut zur Verfügung steht.
Community Cloud	bezeichnet eine Cloud-Infrastruktur, die ausschließlich einer bestimmten Gemeinschaft von Instituten oder Zahlungsinstituten, einschließlich mehrerer Institute einer einzigen Gruppe, zur Verfügung steht.
Hybrid Cloud	bedeutet Cloud-Infrastruktur, die aus zwei oder mehreren unterschiedlichen Cloud-Infrastrukturen besteht.
Leitungsorgan Geschäftsleitung ggf. Senior Management oder Aufsichtsorgan	bezeichnet das Organ oder die Organe eines Instituts oder Zahlungsinstituts, das (die) nach nationalem Recht bestellt wurde (wurden) und befugt ist (sind), Strategie, Ziele und Gesamtpolitik des Instituts oder Zahlungsinstituts festzulegen und die Entscheidungen der Geschäftsleitung zu kontrollieren und zu überwachen, und dem die Personen, die die Geschäfte des Instituts oder Zahlungsinstituts tatsächlich führen, sowie die Geschäftsleiter und die für die Geschäftsleitung des Instituts zuständigen Personen angehören.
Institutsbezogenes Sicherungssystem	Gemäß Eigenkapitalverordnung (Capital Requirements Regulation – CRR) ist ein IPS (Institutional Protection Schema) eine vertragliche oder satzungsmäßige Haftungsvereinbarung einer Gruppe von Banken, welche die Mitgliedsinstitute absichert und insbesondere ihre Liquidität und Solvenz sicherstellt. Durch Anerkennung eines IPS werden bestimmte für einzelne Banken geltende Aufsichtsanforderungen für die IPS-Mitgliedsinstitute gelockert, ähnlich wie dies bei Unternehmen einer konsolidierten Bankengruppe der Fall ist. Beispiele für institutsbezogene Sicherungssysteme in Deutschland sind: ▪ BVR Institutssicherung ▪ Institutssicherung des DSGV

4.7 Nachgelagerte Umsetzungsaktivitäten

Die Umsetzung einer regulatorischen Anforderung zieht fast immer eine Reihe von zusätzlichen Aktivitäten nach sich.

Solche nachgelagerten Umsetzungsaktivitäten können u.a. sein:

- **Dokumentation** der Umsetzung in der **schriftlich fixierten Ordnung**/im Organisationshandbuch Ihres Instituts gemäß §25a KWG sowie AT 5 und 6 MaRisk

- **Erweiterung** des **Internen Kontrollsystems/der Schlüsselkontrollen** um Kontrollen zur Überprüfung der umgesetzten Anforderung gemäß §25a KWG sowie AT 4.3 MaRisk

- **Datenschutz**konformität – Sind von der Umsetzung auch personenbezogene Daten betroffen, so ist die Einhaltung des geltenden Datenschutzrechts sicherzustellen.

  Betrachten Sie dabei insbesondere die sogenannten Betroffenenrechte (Art. 12 bis 23 EU-DSGVO) und prüfen Sie, ob eine Anpassung des Verarbeitungsverzeichnisses gemäß Artikel 30 EU-DSGVO notwendig ist.

- Erweiterung/Anpassung der **Prüfungsplanung** für die **Interne Revision** gemäß BT 2.3 MaRisk

Prüfen Sie, inwieweit Sie hier ebenfalls aktiv werden müssen. Die genannten Punkte werden von Prüfern i.d.R. immer als erstes angesprochen.

5 Anforderungen im Detail

Title I – Proportionality: group application and institutional protection schemes

1. Proportionality

Norm-Bezug: **I.1. Tz. 18**

Thema:

Proportionalität / Verhältnismäßigkeit der Anforderungsumsetzung in Bezug auf das betriebene Bankgeschäft (Fokus auf das Geschäft des Instituts)

betroffene Funktion(en) / Einheit(en):

- Geschäftsleitung
- Auslagerungsverantwortliche

Anforderung (Originaltext):

Institutions, payment institutions and competent authorities should, when complying or supervising compliance with these guidelines, have regard to the principle of proportionality. The proportionality principle aims to ensure that governance arrangements, including those related to outsourcing, are consistent with the **individual risk profile**, the nature and **business model** of the institution or payment institution, and the **scale and complexity of** their **activities** so that the objectives of the regulatory requirements are effectively achieved.

Öffnungsklausel(n) / Erleichterung(en):

Für mittlere und kleinere Institute ermöglicht die Anwendung des Proportionalitätsprinzips ggf. eine „einfachere“ Umsetzung der Anforderungen aus den EBA Leitlinien zu Auslagerungen.

Handlungsoptionen / Umsetzungshinweise:

Bei der Umsetzung der Anforderungen aus dieser Leitlinie in Bezug auf das Geschäft des Instituts, ist stets die Verhältnismäßigkeit zu beachten. Diese lässt sich aus den folgenden Merkmalen herleiten:

- Risikoprofil des Instituts
- Komplexität des Geschäftsmodells
- Umfang des Geschäftsvolumens

Denken Sie im Hinblick auf die Prüfungsfestigkeit der Anforderungsumsetzung besonders an eine nachvollziehbare Herleitung der Argumentation.

Berücksichtigen Sie dabei, dass die Proportionalität in Bezug auf die Anforderungen an Auslagerungen durch die Vorgaben des Kreditwesengesetzes und der MaRisk eng begrenzt ist:

- Gemäß §25b Abs. 1 KWG muss ein Institut abhängig von Art, Umfang, Komplexität und Risikogehalt einer Auslagerung, wenn sie für die Durchführung von Bankgeschäften, Finanzdienstleistungen oder sonstigen institutstypischen Dienstleistungen wesentlich ist, angemessene Vorkehrungen treffen, um übermäßige zusätzliche Risiken aus der Auslagerung zu vermeiden.

  Somit sind von allen Instituten grundlegende Umsetzungshandlungen zur Steuerung von Auslagerungen durchzuführen.

- Gemäß § 25b Abs. 1 KWG darf eine Auslagerung weder die Ordnungsmäßigkeit der betroffenen Geschäfte und Dienstleistungen noch die Geschäftsorganisation im Sinne des § 25a Abs. 1 beeinträchtigen.

  Insbesondere muss ein angemessenes und wirksames Risikomanagement, welches die ausgelagerten Aktivitäten und Prozesse einbezieht, gewährleistet sein.

- AT 1 Tz. 3 der MaRisk fordert eine so genannte „Proportionalität nach oben“ und enthält die Vorgabe, „Institute, die besonders groß sind oder deren Geschäftsaktivitäten durch besondere Komplexität, Internationalität oder eine besondere Risikoexponierung gekennzeichnet sind, weitergehende Vorkehrungen im Bereich des Risikomanagements zu treffen als weniger große Institute mit weniger komplex strukturierten Geschäftsaktivitäten, die keine außergewöhnliche Risikoexponierung aufweisen.“

  Somit müssen besonders große/komplexe Institute im Einzelfall über die Vorgaben der MaRisk hinausgehen. Die EBA-Vorgaben und die Mindestvorgaben der MaRisk sind grundsätzlich von allen Instituten einzuhalten.

- Der Umfang der Anforderungen wird in den MaRisk gemäß AT 1 Tz. 5 proportional über so genannte Öffnungsklauseln geregelt.

  Im Bereich Auslagerungen ist die wichtigste Öffnungsklausel in AT 9 Tz. 12 enthalten. Demnach hat ein Institut ein zentrales Auslagerungsmanagement lediglich abhängig von der Art, dem Umfang und der Komplexität der Auslagerungsaktivitäten einzurichten.

Tz. 18	**Proportionalität / Verhältnismäßigkeit der Anforderungsumsetzung in Bezug auf das betriebene Bankgeschäft (Fokus auf das Geschäft des Instituts)**
Beurteilung Relevanz:	
☐ JA ☐ NEIN	Begründung (wenn NEIN):
Beurteilung Handlungsbedarf:	
notwendige Umsetzungsaktivitäten:	

Was?	Wer?	Bis wann?

☐ Berücksichtigung in der sfO / im OHB
☐ Berücksichtigung im Kontrollumfeld / IKS
☐ Berücksichtigung bei Maßnahmen zum Datenschutz
☐ Berücksichtigung in der Prüfungsplanung IR

geplantes Umsetzungsdatum:	**geschätzter Umsetzungsaufwand:**

Notizen:

Norm-Bezug: **I.1. Tz. 19**

Thema:

Proportionalität / Verhältnismäßigkeit der Anforderungsumsetzung in Bezug auf aktuelle sowie zukünftige Auslagerungen des Instituts (Fokus auf die Auslagerungen des Instituts)

betroffene Funktion(en) / Einheit(en):

- Geschäftsleitung
- Auslagerungsverantwortliche

Anforderung (Originaltext):

When applying the requirements set out in these guidelines, institutions and payment institutions should take into account the complexity of the outsourced functions, the risks arising from the outsourcing arrangement, the criticality or importance of the outsourced function and the potential impact of the outsourcing on the continuity of their activities.

Öffnungsklausel(n) / Erleichterung(en):

siehe I.1. Tz. 18

Handlungsoptionen / Umsetzungshinweise:

Bei der Umsetzung der Anforderungen aus dieser Leitlinie in Bezug auf vorhandene sowie zukünftige Auslagerungen, ist stets die Verhältnismäßigkeit zu beachten. Diese lässt sich aus den folgenden Merkmalen herleiten:

- Komplexität der ausgelagerten Funktion
- Kritikalität und Wesentlichkeit der ausgelagerten Funktion
- Risiken der Auslagerung
- Auswirkung auf die Geschäftskontinuität

Somit muss zunächst einmal eine Bewertung der Kritikalität bzw. Wesentlichkeit der jeweiligen Auslagerung nach den Vorgaben in Tz. 29-31 der EBA Leitlinien zu Auslagerungen vorgenommen werden. Die Kritikalität ergibt sich dabei aus einer Beurteilung der Auswirkungen auf den Geschäftsbetrieb, wenn die ausgelagerte Funktion nicht oder teilweise nicht zur Verfügung steht bzw. in ihrer Qualität beeinträchtigt ist.

Diese Bewertung der Kritikalität bzw. Wesentlichkeit der jeweiligen Auslagerung entspricht der Risikoanalyse zur Festlegung der Wesentlichkeit einer Auslagerung nach AT 9, Tz. 2 MaRisk.

So wie in den MaRisk die Anforderungen an die Steuerung einzelner Auslagerungen abgestuft sind nach deren Wesentlichkeit bzw. Nicht-Wesentlichkeit, hängen die Anforderungen an die Steuerung einzelner Auslagerungen nach den EBA Leitlinien von deren Kritikalität bzw. Wesentlichkeit ab.

Die in den EBA Leitlinien in Abschnitt 12.2 geforderte Risikoanalyse stellt ein davon unabhängiges ergänzendes Element zur Bestimmung des Risikogehalts von Auslagerungen dar.

Die „EBA-Risikoanalyse“ ist somit unabhängig von der Einstufung einer Auslagerung als kritisch oder wesentlich zu sehen.

Tz. 19	**Proportionalität / Verhältnismäßigkeit der Anforderungsumsetzung in Bezug auf aktuelle sowie zukünftige Auslagerungen des Instituts (Fokus auf die Auslagerungen des Instituts)**

Beurteilung Relevanz:

☐ JA ☐ NEIN	Begründung (wenn NEIN):

Beurteilung Handlungsbedarf:

notwendige Umsetzungsaktivitäten:

Was?	Wer?	Bis wann?

☐ Berücksichtigung in der sfO / im OHB
☐ Berücksichtigung im Kontrollumfeld / IKS
☐ Berücksichtigung bei Maßnahmen zum Datenschutz
☐ Berücksichtigung in der Prüfungsplanung IR

geplantes Umsetzungsdatum:	**geschätzter Umsetzungsaufwand:**

Notizen:

Norm-Bezug: **I.1. Tz. 20**

Thema:

Berücksichtigung der Anforderungen aus den EBA Leitlinien zur internen Governance

betroffene Funktion(en) / Einheit(en):

- Geschäftsleitung
- Auslagerungsverantwortliche
- Compliance

Anforderung (Originaltext):

When applying the principle of proportionality, institutions, payment institutions and competent authorities should take into account the criteria specified in Title I of the EBA Guidelines on internal governance in line with Article 74(2) of Directive 2013/36/EU.

Öffnungsklausel(n) / Erleichterung(en):

Keine

Handlungsoptionen / Umsetzungshinweise:

Art. 74 Abs. 2 der CRD beschreibt das Proportionalitätsprinzip in Bezug auf die Anforderungen der Säule II.

Demnach sind aufsichtsrechtliche Anforderungen angemessen nach Art, Umfang und Komplexität der dem Geschäftsmodell bzw. den Geschäften eines Instituts innewohnenden Risiken zu erfüllen.

Titel I der EBA Leitlinien zur internen Governance präzisiert die Kriterien, nach denen die Aufsichtsbehörden die Proportionalität der Anforderungen gegenüber dem einzelnen Institut einstufen können. Diese sind nachfolgend dargestellt.

Für die Anwendung des Grundsatzes der Verhältnismäßigkeit und zur Sicherstellung einer angemessenen Umsetzung der Anforderungen sollten die Institute und die zuständigen Behörden die folgenden Kriterien berücksichtigen:

a. die Größe in Bezug auf die Bilanzsumme des Instituts und seiner Tochtergesellschaften im Anwendungsbereich des aufsichtlichen Konsolidierungskreis;

b. die geografische Präsenz des Instituts und der Umfang seiner Tätigkeiten in den einzelnen Rechtsordnungen;

c. die Rechtsform des Instituts, einschließlich der Tatsache, ob das Institut zu einer Gruppe gehört, und gegebenenfalls die für die Gruppe vorgenommene Bewertung der Verhältnismäßigkeit;

d. die Tatsache, ob das Institut börsennotiert ist oder nicht;

e. die Tatsache, ob das Institut zur Verwendung von internen Modellen für die Messung der Kapitalanforderungen befugt ist (z. B. der auf internen Beurteilungen basierende Ansatz – IRB-Ansatz);

f. die Art der zugelassenen Tätigkeiten und Dienstleistungen des Instituts (siehe beispielsweise auch Anhang 1 der Richtlinie 2013/36/EU und Anhang 1 der Richtlinie 2014/65/EU);

g. das zugrunde liegende Geschäftsmodell und die Strategie, die Art und Komplexität der Geschäftstätigkeiten und die Organisationsstruktur des Instituts;

h. die Risikostrategie, die Risikoappetit und das tatsächliche Risikoprofil des Instituts, auch unter Berücksichtigung der Ergebnisse der SREP-Kapital- und SREP-Liquiditätsbewertungen;

i. die Beteiligungsverhältnisse und die Finanzierungsstruktur des Instituts;

j. die Art der Kunden (z. B. Privat-, Unternehmenskunden, institutionelle Kunden, Kleinunternehmen, öffentliche Stellen) und die Komplexität der Produkte oder Verträge;

k. die ausgelagerten Tätigkeiten und Vertriebskanäle sowie

l. die bestehenden informationstechnischen Systeme (IT-Systeme), einschließlich der Systeme für einen unterbrechungsfreien Geschäftsbetrieb und der Auslagerung von Tätigkeiten in diesem Bereich.

Handlungsbedarf zu dieser Textziffer besteht ggf. dann, wenn Sie sich bei der Umsetzung einzelner Anforderungen dieser EBA Leitlinien auf das Proportionalitätsprinzip berufen.

Prüfen Sie in diesen Fällen, ob ein Verweis auf die Liste, wie sie in Titel I, Tz. 19 der EBA Leitlinien zur internen Governance vom 26.09.2017 enthalten ist, möglich ist.

Tz. 20	**Berücksichtigung der Anforderungen aus den EBA Leitlinien zur internen Governance**
Beurteilung Relevanz:	
☐ JA ☐ NEIN	Begründung (wenn NEIN):
Beurteilung Handlungsbedarf:	
notwendige Umsetzungsaktivitäten:	

Was?	Wer?	Bis wann?

☐ Berücksichtigung in der sfO / im OHB
☐ Berücksichtigung im Kontrollumfeld / IKS
☐ Berücksichtigung bei Maßnahmen zum Datenschutz
☐ Berücksichtigung in der Prüfungsplanung IR

geplantes Umsetzungsdatum:	**geschätzter Umsetzungsaufwand:**

Notizen:

2. Outsourcing by groups and institutions that are members of an institutional protection scheme

Norm-Bezug: **I.2. Tz. 21**

Thema:

Erfüllung der Anforderungen aus der Eigenkapitalrichtlinie (CRD) bzgl. Governance, Prozessen und Verfahren innerhalb von Institutsgruppen

betroffene Funktion(en) / Einheit(en):

- Geschäftsleitung
- Auslagerungsverantwortliche
- Risikomanagement

Anforderung (Originaltext):

In accordance with Article 109 (2) of Directive2013/36/EU, these guidelines should also apply on a sub-consolidated and consolidated basis, taking into account the prudential scope of consolidation. For this purpose, the EU parent undertakings or the parent undertaking in a Member State should ensure that internal governance arrangements, processes and mechanisms in their subsidiaries, including payment institutions, are consistent, well integrated and adequate for the effective application of these guidelines at all relevant levels.

Öffnungsklausel(n) / Erleichterung(en):

Keine

Handlungsoptionen / Umsetzungshinweise:

Stellen Sie sicher, dass die vorliegenden EBA Leitlinien zu Auslagerungen im Einklang mit Artikel 109 (2) der Eigenkapitalrichtlinie (CRD) stehen und legen Sie dabei grundsätzlich den in Tz. 21 genannten aufsichtsrechtlichen Konsolidierungskreis zugrunde.

In Tz. 21 der Leitlinien zu Auslagerungen wird dabei per Fußnote auf die entsprechenden Vorgaben zum aufsichtsrechtlichen Konsolidierungskreis in der CRR verwiesen.

Insbesondere erfordert dies, dass nicht nur Auslagerungen von Instituten in der Gruppe entsprechend den Vorgaben der EBA Leitlinien zu Auslagerungen gesteuert werden müssen,

sondern auch Auslagerungen anderer gruppenangehöriger Unternehmen, sofern diese Unternehmen Bestandteile des aufsichtsrechtlichen Konsolidierungskreises sind.

Die MaRisk enthalten ähnliche Vorgaben zur Risikosteuerung auf Gruppenebene im Abschnitt AT 4.5 und verweisen dabei auf die Vorgaben in §25a Abs. 3 KWG.

Dabei sind gemäß AT 4.5 Tz. 1 grundsätzlich sowohl konsolidierungspflichtige als auch nicht konsolidierungspflichtige Unternehmen betroffen.

Das übergeordnete Unternehmen hat nach AT 4.5 Tz. 5 angemessene Risikosteuerungs- und Risikocontrolling-Prozess einzurichten, der die gruppenangehörigen Unternehmen einbezieht.

Die Erläuterungen zu AT 4.5 Tz. 1 enthalten dabei Öffnungsklauseln hinsichtlich der konkreten Einbeziehung einzelner Unternehmen, worunter auch das Proportionalitätskriterium fällt.

Darin werden die Institute aufgefordert sicherzustellen, dass eine Umsetzung regulatorischer Anforderungen innerhalb von Institutsgruppen bzw. Mitgliedern eines institutsbezogenen Sicherungssystems einheitlich und gut integriert erfolgen sollte.

Wir verstehen darunter die Anforderung an Institutsgruppen bzw. institutsbezogene Sicherungssysteme, für das Auslagerungsmanagement gruppenweit/systemweit einheitliche Regelungen und Verfahren zu implementieren, die bei Bedarf eine Konsolidierung der Informationen über Auslagerungen (insbes. Auslagerungsrisiken) ermöglichen.

Damit können dann Aussagen über das Auslagerungsrisiko sowohl auf Ebene einzelner Gruppenmitglieder, auf Ebene von Teilgruppen (teilkonsolidiert) als auch für die gesamte Institutsgruppe (konsolidiert) getroffen werden.

In der Umsetzungspflicht sieht die EBA hier die „Gruppenmütter“ (Zentralorganisationen) egal ob es sich um EU-Gesellschaften (SEs) oder Gesellschaften aus EU-Mitgliedsländern handelt (in Deutschland z.B. AGs oder GmbHs)

Für die „Gruppentöchter“ kann es ggf. Erleichterungen geben.

Diese Möglichkeit besteht immer dann, wenn die zuständige Aufsichtsbehörde eine Ausnahme gemäß Artikel 21 oder 109 (1) CRD in Verbindung mit Artikel 7 CRR für das Institut erteilt hat (siehe dazu auch I.2. Tz. 24).

Vor Beginn Ihres Umsetzungsprojektes sollten Sie den Status Ihres Instituts (Gruppenmitglied und wenn ja Zentralorganisation oder Tochtergesellschaft) prüfen und feststellen, ob es eine Ausnahme gemäß CRD/CRR gibt.

Tz. 21	**Erfüllung der Anforderungen aus der Eigenkapitalrichtlinie (CRD) bzgl. Governance, Prozessen und Verfahren innerhalb von Institutsgruppen**

Beurteilung Relevanz:

☐ JA ☐ NEIN	Begründung (wenn NEIN):

Beurteilung Handlungsbedarf:

notwendige Umsetzungsaktivitäten:

Was?	Wer?	Bis wann?

☐ Berücksichtigung in der sfO / im OHB
☐ Berücksichtigung im Kontrollumfeld / IKS
☐ Berücksichtigung bei Maßnahmen zum Datenschutz
☐ Berücksichtigung in der Prüfungsplanung IR

geplantes Umsetzungsdatum:	**geschätzter Umsetzungsaufwand:**

Notizen:

Norm-Bezug: **I.2. Tz. 22**

Thema:

Spezifische Anforderungen für Institutsgruppen sowie Mitglieder institutsbezogener Sicherungssysteme in Bezug auf Auslagerungen innerhalb der Institutsgruppe / des institutsbezogenen Sicherungssystems

betroffene Funktion(en) / Einheit(en):

- Geschäftsleitung
- Auslagerungsverantwortliche
- Compliance

Anforderung (Originaltext):

Institutions and payment institutions, in accordance with paragraph 21, and institutions that, as members of an institutional protection scheme, use centrally provided governance arrangements should comply with the following:

a. where those institutions or payment institutions have outsourcing arrangements with service providers within the group or the institutional protection scheme, the management body of those institutions or payment institutions retains, also for these outsourcing arrangements, full responsibility for compliance with all regulatory requirements and the effective application of these guidelines;

b. where those institutions or payment institutions outsource the operational tasks of internal control functions to a service provider within the group or the institutional protection scheme, for the monitoring and auditing of outsourcing arrangements, institutions should ensure that, also for these outsourcing arrangements, those operational tasks are effectively performed, including through the receiving of appropriate reports.

Öffnungsklausel(n) / Erleichterung(en):

Keine

Handlungsoptionen / Umsetzungshinweise:

a. Besteht eine Auslagerungsbeziehung zwischen einem auslagernden Institut und einem Service Provider, der ebenfalls Mitglied der Institutsgruppe oder des institutsbezogenen

Sicherungssystems ist, so **verbleibt** die **Verantwortung zur Erfüllung aller aufsichtlichen Anforderungen** weiter **bei der Geschäftsleitung des auslagernden Instituts**.

b. Lagert ein Institut innerhalb einer Institutsgruppe oder eines institutsbezogenen Sicherungssystems die operative Kontrollfunktion (Monitoring; Auditing) für Auslagerungen selbst aus, so ist es weiterhin für die Sicherstellung der Wirksamkeit dieser Kontrollfunktion verantwortlich. Dies erfordert insbesondere die Sicherstellung einer **angemessenen Berichterstattung zur Beurteilung der Wirksamkeit der Kontrollfunktion**.

Die Vorgabe, dass die Verantwortung der Geschäftsleitung nicht auslagerbar ist, enthält auch §25b Abs. 2 KWG sowie AT 9, Tz. 4 MaRisk.

AT 9 Tz. 5 MaRisk fordert, dass auch bei Auslagerungen von Kontrollbereichen und Kernbankbereichen weiterhin eine wirksame Überwachung der von den Auslagerungsunternehmen erbrachten Dienstleistungen gewährleistet sein muss. Zudem beschränkt AT 9 Tz. 5 MaRisk die Auslagerung der Risikocontrolling-Funktion, Compliance-Funktion und internen Revision.

Sofern bereits die Anforderungen gemäß AT 9 Tz. 4 und 5 MaRisk vollständig erfüllt werden, sehen wir keine neuen Anforderungen an die Institute durch Tz. 22 der EBA Leitlinien zu Auslagerungen.

Tz. 22	**Spezifische Anforderungen für Institutsgruppen sowie Mitglieder institutsbezogener Sicherungssysteme in Bezug auf Auslagerungen innerhalb der Institutsgruppe / des institutsbezogenen Sicherungssystems**
Beurteilung Relevanz:	
☐ JA ☐ NEIN	Begründung (wenn NEIN):
Beurteilung Handlungsbedarf:	
notwendige Umsetzungsaktivitäten:	

Was?	Wer?	Bis wann?

☐ Berücksichtigung in der sfO / im OHB
☐ Berücksichtigung im Kontrollumfeld / IKS
☐ Berücksichtigung bei Maßnahmen zum Datenschutz
☐ Berücksichtigung in der Prüfungsplanung IR

geplantes Umsetzungsdatum:	**geschätzter Umsetzungsaufwand:**

Notizen:

Norm-Bezug: **I.2. Tz. 23**

Thema:

Verbleibende Anforderungen auf Einzelinstitutsebene bei zentraler Erfüllung von Einzelvorgaben zur Auslagerungssteuerung in der Gruppe bzw. im Verbund / institutsbezogenen Sicherungssystem

betroffene Funktion(en) / Einheit(en):

- Geschäftsleitung
- Auslagerungsverantwortliche
- Compliance

Anforderung (Originaltext):

In addition to paragraph 22, institutions and payment institutions within a group for which no waivers have been granted on the basis of Article 109 of Directive 2013/36/EU and Article 7 of Regulation (EU) No 575/2013, institutions that are a central body or that are permanently affiliated to a central body for which no waivers have been granted on the basis of Article 21 of Directive 2013/36/EU, or institutions that are members of an institutional protection scheme should take into account the following:

a. where the operational monitoring of outsourcing is centralised (e.g. as part of a master agreement for the monitoring of outsourcing arrangements), institutions and payment institutions should ensure that, at least for outsourced critical or important functions, both independent monitoring of the service provider and appropriate oversight by each institution or payment institution is possible, including by receiving, at least annually and upon request from the centralised monitoring function, reports that include, at least, a summary of the risk assessment and performance monitoring. In addition, institutions and payment institutions should receive from the centralised monitoring function a summary of the relevant audit reports for critical or important outsourcing and, upon request, the full audit report;

b. institutions and payment institutions should ensure that their management body will be duly informed of relevant planned changes regarding service providers that are monitored centrally and the potential impact of these changes on the critical or important functions provided, including a summary of the risk analysis, including legal risks, compliance with regulatory requirements and the impact on service levels, in order for them to assess the impact of these changes;

c. where those institutions and payment institutions within the group, institutions affiliated to a central body or institutions that are part of an institutional protection scheme rely on a central pre-outsourcing assessment of outsourcing arrangements, as referred to in Section 12, each institution and payment institution should receive a summary of the assessment and ensure that it takes into consideration its specific structure and risks within the decision-making process;

d. where the register of all existing outsourcing arrangements, as referred to in Section 11, is established and maintained centrally within a group or institutional protection scheme, competent authorities, all institutions and payment institutions should be able to obtain their individual register without undue delay. This register should include all outsourcing arrangements, including outsourcing arrangements with service providers inside that group or institutional protection scheme;

e. where those institutions and payment institutions rely on an exit plan for a critical or important function that has been established at group level, within the institutional protection scheme or by the central body, all institutions and payment institutions should receive a summary of the plan and be satisfied that the plan can be effectively executed.

Öffnungsklausel(n) / Erleichterung(en):

Möglichkeit zur Zentralisierung der operativen Überwachung von Auslagerungen im Verbund bei Aufrechterhaltung wesentlicher, im Detail festgelegter Steuerungsverfahren im Einzelinstitut.

Handlungsoptionen / Umsetzungshinweise:

Liegt für Ihr Institut keine Ausnahme gemäß Artikel 21 oder 109 (1) CRD in Verbindung mit Artikel 7 CRR vor, so stellen Sie sicher, dass die folgenden zusätzlichen Anforderungen gegenüber Tz. 21 der Leitlinien zu Auslagerungen erfüllt werden:

a. Wenn die operative Überwachung der Auslagerung zentralisiert ist (z.B. im Rahmen einer Rahmenvereinbarung zur Überwachung von Auslagerungsvereinbarungen), sollten Institute sicherstellen, dass zumindest für ausgelagerte kritische oder wichtige Funktionen sowohl eine unabhängige Überwachung des Service Providers als auch eine angemessene Beaufsichtigung durch jedes Institut möglich ist, auch indem sie mindestens einmal jährlich und auf Anfrage der zentralen Überwachungsfunktion Berichte erhalten, die mindestens eine Zusammenfassung der Risikobewertung und der Leistungsüberwachung enthalten. Darüber hinaus sollten Institute von der zentralen Überwachungsfunktion eine Zusammenfassung der relevanten Auditberichte für kritische oder wichtige Auslagerungen und auf Anfrage den vollständigen Auditbericht

erhalten;

b. Die Institute sollten sicherstellen, dass ihr Leitungsorgan ordnungsgemäß über relevante geplante Änderungen in Bezug auf Service Provider, die zentral überwacht werden, und über die möglichen Auswirkungen dieser Änderungen auf die bereitgestellten kritischen oder wichtigen Funktionen informiert wird, einschließlich einer Zusammenfassung der Risikoanalyse, einschließlich rechtlicher Risiken, der Einhaltung der regulatorischen Anforderungen und der Auswirkungen auf die Servicequalität, damit sie die Auswirkungen dieser Änderungen bewerten können;

c. Wenn sich die Institute der Gruppe, die mit einer oder mehreren zentralen Stellen verbunden sind, die Teil einer institutionellen Sicherungseinrichtung sind, auf eine zentrale Pre-Auslagerungs-Bewertung von Auslagerungsvereinbarungen gemäß Abschnitt 12 stützen, sollte jedes Institut eine Zusammenfassung der Bewertung erhalten und sicherstellen, dass es seine spezifische Struktur und seine spezifischen Risiken im Entscheidungsprozess berücksichtigt;

d. Wenn das Register aller bestehenden Auslagerungen gemäß Abschnitt 11 zentral in einer Gruppe oder einem institutionellen Sicherungssystem eingerichtet und geführt wird, sollten die zuständigen Behörden und alle Institute in der Lage sein, ihr individuelles Register unverzüglich zu erhalten. Dieses Register sollte alle Auslagerungen umfassen, einschließlich Auslagerungsvereinbarungen mit Service Providern innerhalb dieser Gruppe oder des institutionellen Sicherungssystems;

e. Wenn diese Institute auf einen Ausstiegsplan für eine kritische oder wichtige Funktion angewiesen sind, der auf Gruppenebene, im Rahmen der institutionellen Sicherungseinrichtung oder durch die Zentraleinrichtung festgelegt wurde, sollten alle Institute eine Zusammenfassung des Plans erhalten und sich davon überzeugen können, dass der Plan wirksam ausgeführt werden kann.

Die Vorgaben in Tz. 23 präzisieren die Anforderungen an die Gesamtverantwortung der Geschäftsleitung im Fall von Auslagerungen im Verbund.

Sie sind deutlich konkreter als die allgemeine Regelung in AT 9 Tz. 4 MaRisk.

Demnach sind die in der Tz. 23 genannten Anforderungen zu erfüllen, sofern für das Institut kein entsprechender Waiver zu den Säule II Anforderungen gemäß Artikel 1009 CRD in Verbindung mit Artikel 7 CRR vorliegt und dennoch eine zentralisierte Erfüllung einzelner Vorgaben im Auslagerungsmanagement erfolgt (z.B. die zentrale Führung eines Auslagerungsregister oder gemeinschaftliche Erstellung eines Ausstiegsplan).

Tz. 23 ermöglicht eine zentrale Überwachung von Auslagerungsunternehmen im Verbund (d.h. in der Institutsgruppe oder im institutsbezogenen Sicherheitsverbund, sofern eine „retained organisation“ bezüglich der Steuerung der Auslagerungen weiterhin im Institut vorliegt.

Insofern kann Tz. 23 der Leitlinien zu Auslagerungen als Checkliste dienen, was zu beachten ist, sofern die operative Überwachung der Auslagerungen im Institut zentralisiert wird.

Tz. 23	**Verbleibende Anforderungen auf Einzelinstitutsebene bei zentraler Erfüllung von Einzelvorgaben zur Auslagerungssteuerung in der Gruppe bzw. im Verbund / institutsbezogenen Sicherungssystem**
Beurteilung Relevanz:	
☐ JA ☐ NEIN	Begründung (wenn NEIN):
Beurteilung Handlungsbedarf:	
notwendige Umsetzungsaktivitäten:	

Was?	Wer?	Bis wann?

☐ Berücksichtigung in der sfO / im OHB
☐ Berücksichtigung im Kontrollumfeld / IKS
☐ Berücksichtigung bei Maßnahmen zum Datenschutz
☐ Berücksichtigung in der Prüfungsplanung IR

geplantes Umsetzungsdatum:	**geschätzter Umsetzungsaufwand:**

Notizen:

Norm-Bezug: **I.2. Tz. 24**

Thema:

Ebene für die Erfüllung der Anforderungen aus den EBA Leitlinien zu Auslagerungen bei Vorliegen einer Ausnahme gemäß Artikel 21 oder 109 (1) CRD in Verbindung mit Artikel 7 CRR für das Institut

betroffene Funktion(en) / Einheit(en):

- Geschäftsleitung
- Auslagerungsverantwortliche
- Compliance

Anforderung (Originaltext):

Where waivers have been granted pursuant to Article 21 of Directive 2013/36/EU or Article 109(1) of Directive 2013/36/EU in conjunction with Article 7 of Regulation (EU) No 575/2013, the provisions of these guidelines should be applied by the parent undertaking in a Member State for itself and its subsidiaries or by the central body and its affiliates as a whole.

Öffnungsklausel(n) / Erleichterung(en):

Prüfen Sie, ob für Ihr Institut eine Befreiung (Waiver) gemäß Artikel 21 (ständige Zuordnung zu einer Zentralorganisation) oder 109 (1) CRD in Verbindung mit Artikel 7 CRR von der Aufsichtsbehörde gewährt wurde.

In diesem Fall sind die Anforderungen der EBA Leitlinien zu Auslagerungen (lediglich) auf Gruppenebene (konsolidiert) bzw. von der Zentralorganisation gemäß Art. 10 CRR zu erfüllen.

Die Beantragung der Befreiung nach Art. 7 CRR, der auch von der Erfüllung der Vorgaben von §25a KWG, den MaRisk und den BAIT befreien kann, ist im deutschen Aufsichtsrecht in §2a Abs. 1 KWG geregelt.

Handlungsoptionen / Umsetzungshinweise:

Siehe Öffnungsklausel(n) / Erleichterungen

Tz. 24	**Ebene für die Erfüllung der Anforderungen aus den EBA Leitlinien zu Auslagerungen bei Vorliegen einer Ausnahme gemäß Artikel 21 oder 109 (1) CRD in Verbindung mit Artikel 7 CRR für das Institut**

Beurteilung Relevanz:

☐ JA ☐ NEIN	Begründung (wenn NEIN):

Beurteilung Handlungsbedarf:

notwendige Umsetzungsaktivitäten:

Was?	Wer?	Bis wann?

☐ Berücksichtigung in der sfO / im OHB
☐ Berücksichtigung im Kontrollumfeld / IKS
☐ Berücksichtigung bei Maßnahmen zum Datenschutz
☐ Berücksichtigung in der Prüfungsplanung IR

geplantes Umsetzungsdatum:	**geschätzter Umsetzungsaufwand:**

Notizen:

Norm-Bezug: **I.2. Tz. 25**

Thema:

Ebene für die Erfüllung der Anforderungen aus den EBA Leitlinien zu Auslagerungen, wenn keine Ausnahme gemäß Artikel 21 oder 109 (1) CRD in Verbindung mit Artikel 7 CRR für das Institut vorliegt

betroffene Funktion(en) / Einheit(en):

- Geschäftsleitung
- Auslagerungsverantwortliche
- Compliance

Anforderung (Originaltext):

Institutions and payment institutions that are subsidiaries of an EU parent undertaking or of a parent undertaking in a Member State to which no waivers have been granted on the basis of Article 21 of Directive 2013/36/EU or Article 109(1) of Directive 2013/36/EU in conjunction with Article 7 of Regulation (EU) No 575/2013 should ensure that they comply with these Guidelines on an individual basis.

Öffnungsklausel(n) / Erleichterung(en):

Keine

Handlungsoptionen / Umsetzungshinweise:

Sollte für Ihr Institut keine Ausnahme gemäß Artikel 21 oder 109 (1) CRD in Verbindung mit Artikel 7 CRR vorliegen, so sind die Anforderungen aus den EBA Leitlinien zu Auslagerungen innerhalb der Institutsgruppe von allen Gruppenmitgliedern einzeln zu erfüllen.

Diese Vorgabe entspricht den Regelungen gemäß §25b KWG und AT 2.1 Tz. 1 MaRisk, wonach die Anforderungen an die Steuerungen an alle Institute gerichtet sind (und darüber hinaus gemäß AT 2.1 Tz. 2 in Teilen auch an Finanzdienstleistungsinstitute und Wertpapierhandelsbanken)

Tz. 25	**Ebene für die Erfüllung der Anforderungen aus den EBA Leitlinien zu Auslagerungen, wenn <u>keine Ausnahme</u> gemäß Artikel 21 oder 109 (1) CRD in Verbindung mit Artikel 7 CRR für das Institut vorliegt**
Beurteilung Relevanz:	
☐ JA ☐ NEIN	Begründung (wenn NEIN):
Beurteilung Handlungsbedarf:	
notwendige Umsetzungsaktivitäten:	

Was?	Wer?	Bis wann?

☐ Berücksichtigung in der sfO / im OHB
☐ Berücksichtigung im Kontrollumfeld / IKS
☐ Berücksichtigung bei Maßnahmen zum Datenschutz
☐ Berücksichtigung in der Prüfungsplanung IR

geplantes Umsetzungsdatum:	**geschätzter Umsetzungsaufwand:**

Notizen:

6 Über die Autoren

In diesem Abschnitt möchten wir uns Ihnen gerne kurz vorstellen.

Dr. Patrik Buchmüller

Patrik Buchmüller war als Mitarbeiter der BaFin zuständig für die Umsetzung der Basel II Vorgaben zum operationellen Risiko (OpRisk) in das nationale Aufsichtsrecht und Mitglied der OpRisk-Gruppe des Baseler Ausschusses sowie weiterer nationaler und internationaler Arbeitsgruppen der Bankenaufsicht.

Er besitzt langjährige Erfahrung als Risikomanager im öffentlichen und privaten Bankensektor. Aktuell beschäftigt er sich als Unternehmensberater mit Umsetzungsfragen zu MaRisk und BAIT.

Patrik Buchmüller ist Autor zahlreicher Fachpublikationen (u.a. Interpretationsleitfaden zur 5. MaRisk-Novelle und diverse Kommentierungen der Vorgaben von CRR und KWG) sowie regelmäßiger Referent bei Fachtagungen und Hochschuldozent zu den Themen IT-Risiko und IT-Recht.

Oliver Rambock

Oliver Rambock war Mitarbeiter eine großen internationalen Universalbank, bevor er in die Unternehmensberatung wechselte.

Seit über 15 Jahren berät er Banken, Sparkassen und Kapitalverwaltungsgesellschaften in den Themenfeldern Risikomanagement und Regulatorik. Aktuelle Schwerpunkte seiner Beratungstätigkeiten bilden die Themen Regulatorik von Auslagerungen sowie IT-Risikomanagement und IT-Sicherheit.

Oliver Rambock ist Mitglied der Global Association of Risk Professionals (GARP) sowie der International Project Management Association (IPMA).

Als Autor und Referent beschäftigt er sich seit Jahren intensiv mit Konzepten und Methoden zur Wissensvermittlung. Um die Möglichkeiten digitaler Bildungsangebote mit den Themen Risikomanagement und Regulatorik zu verbinden, hat er die MARISK ACADEMY gegründet.

7 Kontaktdaten

Sollten Sie Fragen zum Thema Auslagerungen haben oder Anregungen zur Weiterentwicklung unserer Arbeitsbuchs, senden Sie uns eine E-Mail an die folgende Adresse:

support@marisk.academy

8 Druckvorlagen

In diesem Abschnitt finden Sie zwei Druckvorlagen.

Die erste Vorlage können Sie verwenden, wenn Sie weitere eigene Anforderungen im Rahmen Ihres Umsetzungsprojektes berücksichtigen wollen.

Die zweite Druckvorlage stellt Ihnen den Umsetzungsplan ohne Titelbeschriftung zur Verfügung. Nutzen Sie diese Vorlagen, wenn Sie die Umsetzung eigener Anforderungen planen möchten oder wenn Sie mehr Platz bei der Umsetzungsplanung für einzelne regulatorische Anforderungen benötigen.

8.1 Anforderung

Auf der folgenden Seite stellen wir Ihnen das Formular zum Ausdrucken zur Verfügung.

Identifier	Thema
betroffene Funktion(en) / Einheit(en):	
Anforderung:	
Handlungsoptionen / Umsetzungshinweise	
Notizen:	

8.2 Umsetzungsplanung

Auf der folgenden Seite finden Sie die Druckvorlage.

Bezug	**Thema**
Beurteilung Relevanz:	
☐ JA ☐ NEIN	Begründung (wenn NEIN):
Beurteilung Handlungsbedarf:	
notwendige Umsetzungsaktivitäten:	

Was?	Wer?	Bis wann?

☐ Berücksichtigung in der sfO / im OHB
☐ Berücksichtigung im Kontrollumfeld / IKS
☐ Berücksichtigung bei Maßnahmen zum Datenschutz
☐ Berücksichtigung in der Prüfungsplanung IR

geplantes Umsetzungsdatum:	**geschätzter Umsetzungsaufwand:**
Notizen:	