ORO
make regulation work

Whitepaper

Dienstleistungsmanagement im Fokus der Aufsicht

ORO Services GmbH, Hansa Haus, Berner Str.74 , 60437 Frankfurt am Main,

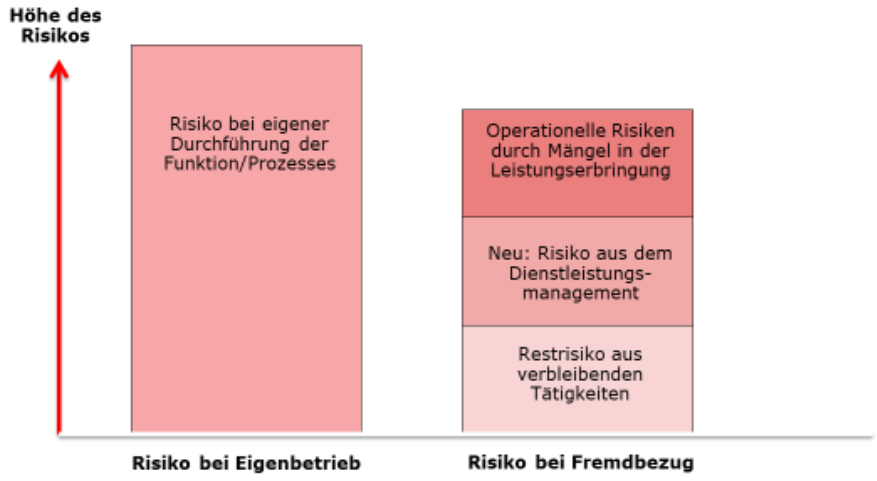
Inhaltsverzeichnis

1. Ausgangslage – Das Dienstleistungsmanagement im Fokus der Aufsicht

Häufig wird das Dienstleistungsmanagement nur rein singulär und nicht im Kontext betrachtet. Der Fokus liegt oft auf der Handhabung der einzelnen Leistungserbringung und nicht auf dem Gesamtkontext aller Dienstleistungen, deren Abhängigkeiten und Verknüpfungen im Prozessgefüge des beauftragenden Unternehmens. Dabei ist die gesamthafte Perspektive und das umfassende Management für die Strategie, das Risikomanagement und letztendlich für den materiellen und wirtschaftlichen Erfolg von Auslagerungen und Dienstleistungen von entscheidender Bedeutung.

Der vermeintliche Kosten-, Know-How- oder Geschwindigkeitsvorteil kann sich schnell ins Gegenteil verkehren, wenn nicht ein ganzheitliches Dienstleistungsmanagement betrieben wird. Dabei wird der administrative oder regulatorische Aufwand für eine Leistungserbringung oder auch mögliche Qualitätsprobleme bei der Dienstleistung, die erwünschten Vorteile rasch aushebeln. Jede Dienstleistung durch einen Dritten verändert damit auch die Risikopositionen des Auftraggebers.

Make or buy? Auch die Risikosituation verändert sich....



Aufsichtsbehörden formulieren Handlungsbedarf

Auch die nationale und internationale Aufsicht ist auf diese Sachverhalte aufmerksam geworden und hat in der Vergangenheit mit Regularien und mit Prüfungen auf die zunehmende Tendenz des Finanzsektors zum Drittbezug von Dienstleistungen reagiert. Die Anzahl an Auslagerungen und externen Dienstleistern, die sich bei einem durchschnittlichen Institut ergibt, ist mitunter sehr groß und kann schnell im 3-stelligen Bereich liegen.

Vermehrt stellt die Aufsicht die oben schon genannten Probleme im Dienstleistungsmanagement durch die Finanzinstitute fest. Hinzu kommt eine wachsende Anzahl von Angriffen auf IT-Strukturen, Intransparenz bei Sub-Dienstleistern oder Klumpen-Risiken durch Beauftragung weniger, teils oligopolistischer Anbieter.

Mängel im Dienstleistungsmanagement oder beim Dienstleister werden bei Prüfungen häufig mit F3 oder F4 (schwerwiegende Mängel) moniert. Auch zum Teil erhebliche Zuschläge auf die Risikovorsorge sind die Folgen für die Institute.

Als weitere Konsequenzen verschärfen nun eine ganze Reihe neuer regulatorische Vorgaben den Druck auf das Management erheblich. Neben den MaRisk und BAIT, stellen insbesondere die EBA Guidelines hohe Anforderungen an die Dienstleistersteuerung bzw. an das auslagerungswillige Institut. Zusätzlich verstärkt werden diese durch das kommende FISG (Gesetz zur Stärkung der Finanzmarktintegrität). Hierbei ist von Bedeutung, dass es zunächst unerheblich ist, ob ein sonstiger Fremdbezug, eine unwesentliche Auslagerung oder eine wesentliche Auslagerung vorliegt. Etliche Vorschriften betreffen alle drei Dienstleistungsformen.

1.1 Sonstiger Fremdbezug oder Auslagerung?

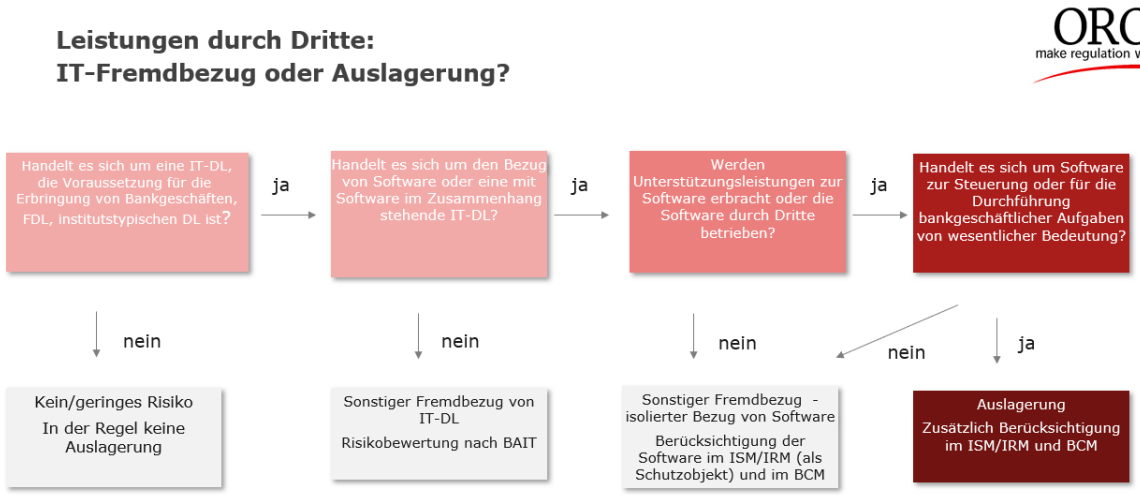
Im Rahmen einer Analyse muss ein Finanzinstitut beurteilen, ob es sich bei einer IT-Dienstleistung durch einen Dritten um einen IT-Fremdbezug oder um eine Auslagerung handelt. Das ist häufig nicht immer eindeutig, und viele Institute tun sich schwer mit der eindeutigen Festlegung. Dabei ist die Definition darüber, wann eine Auslagerung vorliegt und wann ein sonstiger Fremdbezug, klar beschrieben.

Wann liegt eine Auslagerung vor?

Eine Auslagerung i.S.v. §25b Abs. 1 KWG i.V.m. AT 9 Tz. 1 MaRisk liegt vor, wenn ein anderes Unternehmen mit der Wahrnehmung solcher Aktivitäten und Prozesse im Zusammenhang mit der Durchführung von Bankgeschäften, Finanzdienstleistungen oder sonstigen institutstypischen Dienstleistungen beauftragt wird, die ansonsten vom Institut selbst erbracht würden.

Bei Software, die zur Identifizierung, Beurteilung, Steuerung, Überwachung und Kommunikation von Risiken eingesetzt wird oder die für die Durchführung von bankgeschäftlichen Aufgaben von wesentlicher Bedeutung ist, stellen die nachfolgenden Unterstützungsleistungen sowie der Betrieb der Software eine Auslagerung dar:

- die Anpassung der Software an die Erfordernisse des Instituts,
- die entwicklungstechnische Umsetzung von Änderungswünschen (Programmierung),
- das Testen, die Freigabe und die Implementierung der Software in die Produktionsprozesse beim erstmaligen Einsatz und bei wesentlichen Veränderungen insbesondere von programmtechnischen Vorgaben,
- Fehlerbehebungen (Wartung) gemäß der Anforderungs-/Fehlerbeschreibung des Auftraggebers oder des Herstellers oder
- sonstige Unterstützungsleistungen, die über die reine Beratung hinausgehen.



Sonstiger Fremdbezug fällt künftig in das Aufgabengebiet des Auslagerungsmanagements

Doch selbst wenn es sich tatsächlich „nur" um einen sonstigen IT-Fremdbezug handelt, sind die Anforderungen an den Umgang durch das Institut diesbezüglich nach dem Entwurf der neuen BAIT (9. Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen) ebenfalls sehr hoch. So muss das Institut anhand einer Risikobewertung vorab bewerten, welche Risiken mit dem Fremdbezug von IT-Dienstleistungen verbunden sind. Die Ergebnisse der Risikoverortung müssen in die operationellen Risiken der Steuerung einfließen.

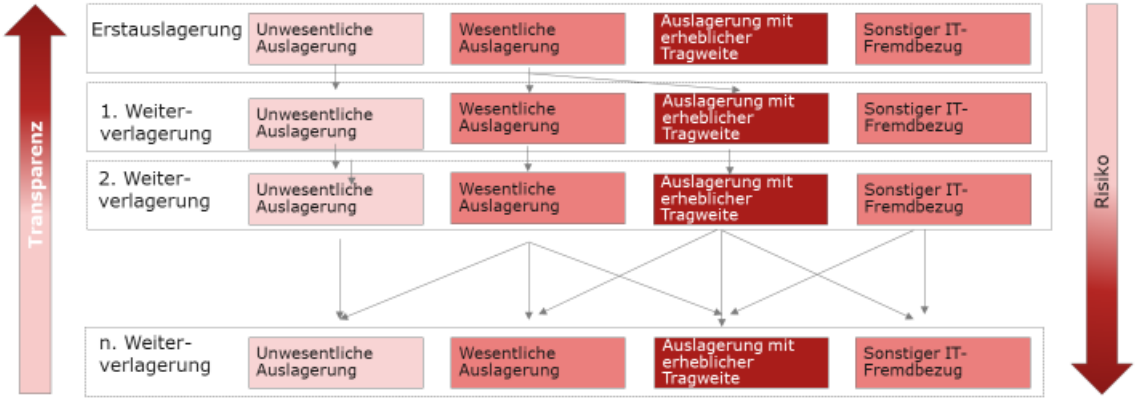
Die Aufsicht erwartet eine Aufgabenerweiterung des Auslagerungsmanagements bzw. des zentralen Auslagerungsmanagers um das Management des sonstigen Fremdbezugs. So muss künftig eine vollständige Aufstellung und Risikobewertung des sonstigen Fremdbezugs von IT-Dienstleistungen erfolgen und dies ist auch regelmäßig zu überwachen. Auch die interne Revision muss ihre Prüfungen auf das Risikomanagement des sonstigen Fremdbezugs erweitern.

Insofern werden die Anforderungen auch an das Risikomanagement des sonstigen IT-Fremdbezugs in Zukunft weiter steigen. Man kann eigentlich schon fast davon ausgehen, dass dies kurzfristig in der Prüfungspraxis ähnlich bewertet wird wie die Anforderungen an die Auslagerung. Daher wird im Folgenden nicht mehr auf die Differenzierung eingegangen.

1.2 Problem: Dienstleistungsketten

In der Praxis bleibt es nicht immer bei einer reinen 1:1 Beziehungskette zwischen Dienstleister und Institut. Die primären Dienstleistungsunternehmen versuchen ihre operativen Tätigkeiten sowie ihre Kosten ebenfalls durch weiteren Leistungsbezug durch Sub-Unternehmen zu optimieren. Hierdurch bilden sich Dienstleistungsketten. Das auslagernde Institut bleibt selbstverständlich auch im Falle der Weiterverlagerung für die Ordnungsmäßigkeit der ausgelagerten Aktivitäten verantwortlich, wobei es unerheblich ist, über wie viele Ebenen weiterverlagert wird. Die nachfolgende Abbildung zeigt ein Beispiel möglicher Konstellationen von Dienstleisterketten:

Erhöhtes Risiko durch Auslagerungsketten



Auslagerungsketten lösen eine ganze Reihe von Fragestellungen und Problemen aus, die zu klären sind:

- Mit zunehmender Weiterverlagerungstiefe sinken die Informationsflüsse einschließlich der Einschätzung, ob die jeweiligen Informationen noch angemessen sind.
- Die wachsende Komplexität erschwert die Transparenz, wie der Prozess auf die verschiedenen Dienstleistungsebenen „verteilt" ist, d. h. was die jeweiligen Aus- bzw. Weiterverlagerungsgegenstände sind (Wer ist für Was verantwortlich?).
- Alle Anforderungen und Regelungen, die das Institut mit seinem primären Dienstleister vereinbart hat, müssen auch für die weiteren Sub-Dienstleister gelten, z.B. Prüfungsrechte SLAs, Reportpflichten, Notfallkonzepte etc.

2. Organisation, Framework und Prozesse

Um ein funktionierendes Dienstleistungsmanagement zu implementieren und zu leben, benötigt es ein Zusammenspiel von Organisation, Frameworks und Regelungen sowie revolvierenden Prozessen.

Organisation, Prozesse und Framework bilden das Auslagerungsmanagement

- Aufbau- und Ablauforganisation bilden zusammen mit einem grundlegenden Framework, wie der Outsourcingstrategie und weiteren Regelungen, das Auslagerungsmanagement.
- Die Kern-Prozesse des Auslagerungsmanagement sind regelmäßig oder anlassbezogen zu durchlaufen.

2.1 Organisation

Operating Modell

Zu einem funktionsfähigen Auslagerungsmanagement gehört das Mitwirken nahezu der gesamten Organisation des Instituts. Der Vorstand in seiner letztendlichen, nicht deligierbaren Verantwortung muss zunächst die (Outsourcing-) Strategie festlegen und mit konkreten Zielen verankern. Er ist auch die letzte Entscheidungsinstanz, wenn es um Auslagerungsentscheidungen oder -maßnahmen geht.

Die dezentralen Auslagerungsbeauftragten sind in der Regel die jeweiligen Fachbereiche, die die Auslagerung betreiben (Kredit, Wertpapier, Kundenberatung, Zahlungsverkehr, IT etc.). Ihnen obliegt die operative Steuerung und Überwachung der jeweiligen Dienstleister.

Zentrales Auslagerungsmanagement

Die Aufsicht fordert, dass ein zentraler Auslagerungsbeauftragter benannt ist, der ggf. durch ein zentrales Auslagerungsmanagement unterstützt werden muss. Somit hat eine Stelle im Unternehmen einen Gesamtüberblick über alle ausgelagerten Aktivitäten und Prozesse und das Unternehmen kann einen möglichst einheitlichen Umgang mit den besonderen Risiken aus Auslagerungen und deren Überwachung sicherstellen.

Die Aufgaben, für die der Auslagerungsbeauftragte bzw. das zentrale Auslagerungsmanagement (ZAM) zuständig sind, sind anspruchsvoll:

_Steuerung, Überwachung und Kontrolle aller Auslagerungen auf übergeordneter Ebene

_Setzen von instituts- und gruppenweit gültigen Standards (Vorgaben)

_Vertragsmanagement

_Regelmäßige Berichterstattung an den Vorstand

_Steuerung und Überwachung der einzelnen Auslagerung

_Steuerung und Bewertung des Risikos, einzeln und gesamtbetrachtet

_Reporting

_Durchführung der Kostenkontrolle

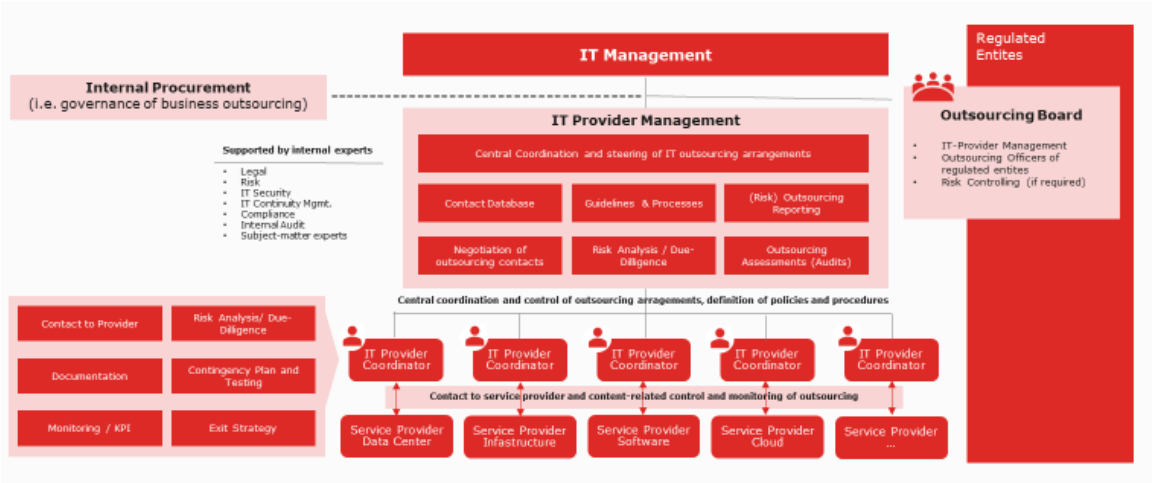
_Monitoring Business Case der Auslagerungen

_Monitoring SLA/KPI und Maßnahmeneinleitung bei Schlechtleistung

_Exit- und Notfallpläne der ausgelagerten Prozesse

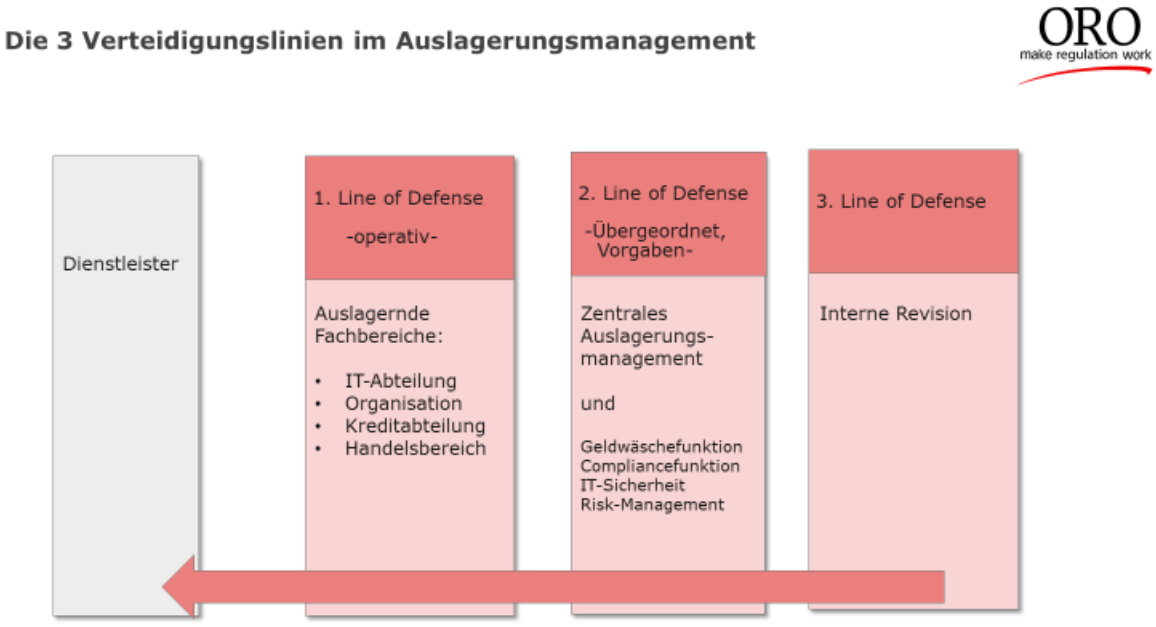
Bei dieser Fülle von Aufgaben und Pflichten im ZAM wird schnell klar, dass die fachliche und persönliche Qualifikation des Auslagerungsbeauftragten bzw. des ZAM eine große Herausforderung darstellt.

Projektbeispiel – Aufbau eines Auslagerungsmanagements bei einem regulierten Institut



Die 3 Lines of Defense

Die MaRisk fordert den Aufbau interner Kontrollverfahren, welche sich wiederum aus dem Internen Kontrollsystem (Linie 1 und 2) und der Internen Revision (Linie 3) zusammensetzen. Die Aufgabe des Internen Kontrollsystems ist die Kontrolle der (ausgelagerten) Prozesse und Überwachungsaufgaben. Die Kontrollen dienen dem Ziel, Fehler, Schwachstellen und Mängel im Dienstleistungsprozess transparent zu machen. Die Aufgabe der Internen Revision ist es hingegen, die Wirksamkeit des Internen Kontrollsystems des Instituts und das des Dienstleisters zu beurteilen. Insofern muss ein Dienstleister – und seine Sub-Dienstleister - also auch immer selbst ein Internes Kontrollsystem haben und diesbezügliche Berichte zur Verfügung stellen. Gegebenenfalls kann dies auch durch eine externe Zertifizierung (s. weiter unten) erfolgen.



2.2 Framework/Governance

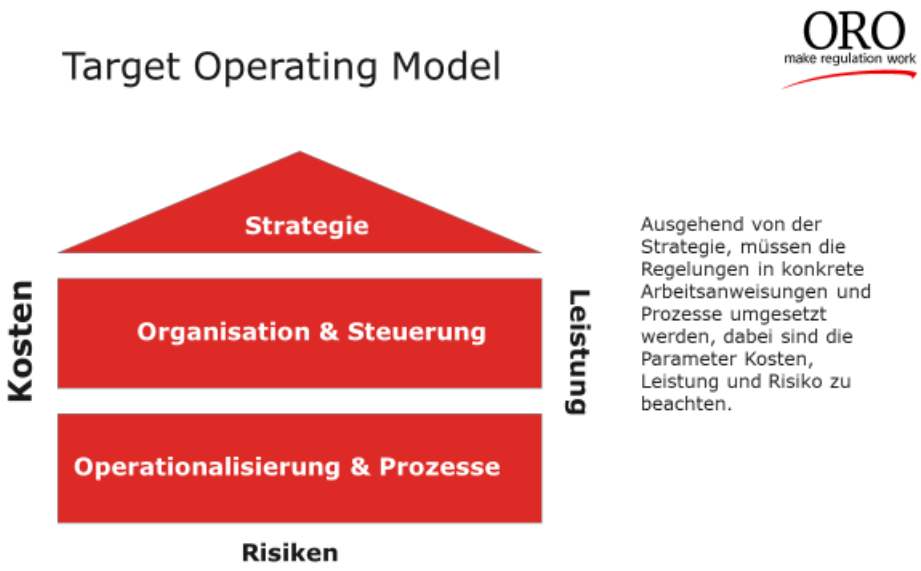
Neben den organisatorischen Vorrausetzungen, müssen auch eine entsprechende Governance-Struktur und ein Regelwerk eingerichtet werden. Dies umfasst neben der grundlegenden Outsourcing-Strategie, die vom Vorstand vorgegeben wird, auch diverse Policies und Regelungen bis hin zu einzelnen konkreten Anweisungen.

Institute müssen alle Risiken aus Vereinbarungen mit Externen – übrigens unabhängig davon, ob es sich dabei um Auslagerungen handelt oder nicht (!!!) – identifizieren, beurteilen, steuern und überwachen müssen, dies stellt gemäß den EBA Leitlinien zum Outsourcing eine grundlegende Anforderung an die neuen Governance-Rahmenwerke dar. Dazu gehören auch klare organisatorische Regelungen in der umfassenden „Outsourcing-Policy", wie die Definitionen von Grundsätzen, Risikoleitplanken, Zuständigkeiten und Prozessen.

Outsourcing-Strategie

Oftmals sind Lieferantenbeziehungen historisch gewachsen und jede individuelle Sourcing-Entscheidung ist oft für sich eher aufgrund taktischer Überlegungen zur jeweiligen Zeit getroffen worden. Strategische Überlegungen wurden dabei jedoch meist vernachlässigt. Häufig erwachsen aus eben diesem Fehlen einer übergeordneten Strategie sowohl ein hoher Steuerungsaufwand als auch eine geringe Interoperabilität dieser Lieferantenbeziehungen zueinander - im schlimmsten Falle verfolgen verschiedene Lieferanten sogar unterschiedliche Zielsetzungen. Daher fordert die Aufsicht von den Instituten einen Bauplan in Form einer Sourcing-Strategie. Zu beachten ist jedoch, dass die Strategie auch hinreichend konkrete Angaben enthält, deren Erfüllungsgrad messbar ist. Nach dem Motto: „Measure it – or forget it!" Wesentliche Bestandteile einer Outsourcing-Strategie sind:

- Strategische Ziele beim Outsourcing: Kostenreduzierung, Qualitätssteigerung, Effizienzgewinn,…
- Art und Umfang von Auslagerungen, die einzelnen Geschäftsfelder/Prozesse betreffend
- Maximaler tolerierter Grad an Weiterverlagerungen
- Datenschutz- und IT-Sicherheitsleitlinien
- Risikotoleranz und Umgang mit: Verlust von KnowHow, operationellen Risiken, Abhängigkeiten vom Dienstleister, Kundenakzeptanz)
- Standort der Leistungserbringung (Onshore, Nearshore, Offshore)
- Single- vs. Multi-Provider-Strategie



Outsourcingsrichtlinien und Arbeitsanweisungen

Diese Dokumentationen haben mehrere Funktionen. Zum einen sollen sie Mitarbeitern und Verantwortlichen klare Hilfestellungen und Handlungsmaßnahmen geben, zum anderen dienen sie bei Prüfungen dem Nachweis der Ordnungsmäßigkeit der Abläufe und Organisationen. Alle Dokumentationen müssen regelmäßig überprüft und ggf. aktualisiert werden. Folgende Angaben sollten in den Richtlinien/Anweisungen enthalten sein:

_Beschreibung der relevanten rechtlichen Ausgangslage

_Begriffe, Definitionen und Abgrenzungen (z.B. Wesentlichkeit)

_Auslagerungsrelevanter Pflichtenkatalog

_Interne Verantwortlichkeiten, Entscheidungswege

_Rahmenvorgaben für Auslagerungsverträge

_Risikoanalyseprozess (Ablauf und Beteiligte)

_Anlass/Prozess für Aktualisierung der Risikoanalysen

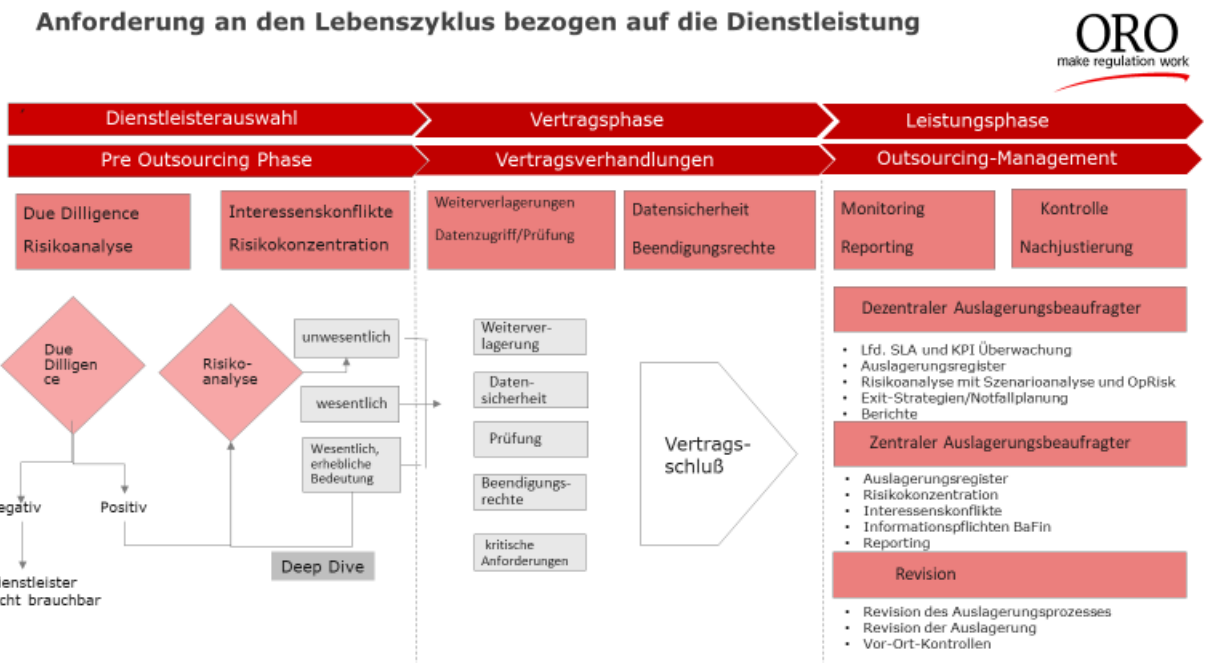
_Internes Reporting

_Monitoring der Dienstleister

_Notfallplanung

2.2 Prozesse

Das Dienstleistungsmanagement beinhaltet eine Reihe bedeutender Kernprozesse, die sich anlassbezogen und/oder turnusmäßig wiederholen. Die hierbei wesentlichen Prozesse werden in den folgenden Kapiteln beschrieben.



2.3.1 Auslagerungsregister

Künftig ist ein vollständiges und aktuelles Register durch das Institut zu führen, welches sämtliche Auslagerungstatbestände umfasst, auch die Unwesentlichen. Ziel der Aufsicht ist es, u.a. Risiken aus der Bündelung von Auslagerungen zu erkennen. Risiken können sich entweder dadurch ergeben, dass ein Institut eine Vielzahl von Prozessen und Funktionen auf denselben Dienstleister auslagert oder, dass viele Banken auf ein und denselben Dienstleister auslagern.

Das Register muss mindestens die folgenden Informationen für alle bestehenden Auslagerungsvereinbarungen enthalten:

- Referenznummer für jede Auslagerungsvereinbarung
- Beginndatum, Datum der nächsten Vertragsverlängerung, das Datum des Endes und/oder Kündigungsfristen
- Kurzbeschreibung der ausgelagerten Funktion
- Daten sowie Angaben darüber, ob personenbezogene Daten betroffen sind
- Kategorie der ausgelagerten Funktion (z. B. IT, Kontrollfunktionen)
- Name des Dienstleisters, Handelsregisternummer, Rechtsträgerkennung (LEI), Adresse und sonstige Kontaktangaben sowie ggf. der Name des Mutterunternehmens.
- Das Land bzw. die Länder, in dem/denen der Dienst erbracht werden soll
- Handelt es sich um eine kritische oder wesentliche ausgelagerte Funktion (inkl. Kurzer Begründung)?
- Bei der Auslagerung zu einem Cloud-Anbieter sind das Cloud-Dienstmodell und das Cloud-Bereitstellungsmodell, d. h. die öffentliche/private/Hybrid- oder Community-Cloud zu nennen

Bei der Auslagerung von kritischen oder wesentlichen Funktionen muss das Register zudem noch folgende zusätzliche Informationen enthalten:

- Datum der letzten Risikobewertung und eine kurze Ergebniszusammenfassung
- Person oder Entscheidungsgremium (z. B. das Leitungsorgan), welches die Auslagerungsvereinbarung genehmigt hat
- Geltendes Recht der Vereinbarung
- Datum der letzten und der nächsten geplanten Prüfung
- Namen von Subunternehmern, an die wesentliche Teile einer kritischen oder wesentlichen Funktion weiter ausgelagert werden
- Ersetzbarkeit des Dienstleisters (leicht, schwierig oder unmöglich)
- Möglichkeit einer Wiedereingliederung oder Auswirkungen bei Einstellung der kritischen oder wesentlichen Funktion
- Alternative Dienstleister
- Angaben, ob zeitkritische Funktionen betroffen sind
- Veranschlagtes jährliches Budget bzw. Kosten

2.3.2 Vertragsmanagement

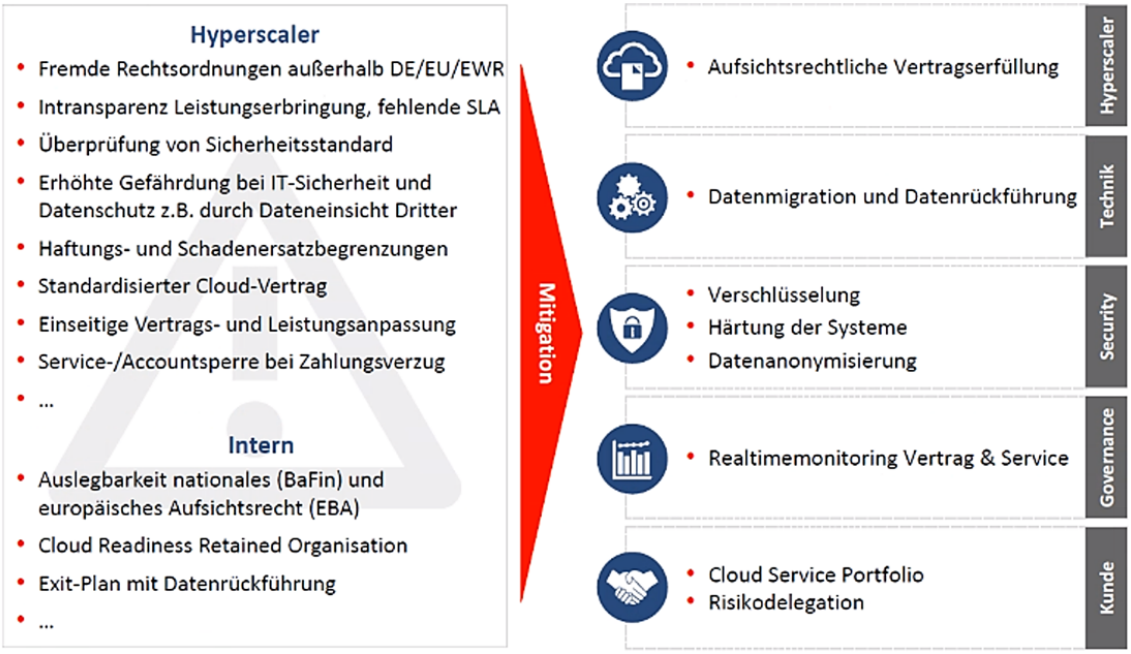
Im Auslagerungsvertrag mit dem Dienstleister und den jeweiligen Sub-Dienstleistern sind bestimmte Klauseln zu fixieren.

Bei wesentlichen Auslagerungen sind die Weisungsrechte des auslagernden Instituts vertraglich festzulegen. Mit einer bedeutenden Ausnahme: Wenn die vom Auslagerungsunternehmen respektive Mehrmandantendienstleister zu erbringende Leistung hinreichend klar im Auslagerungsvertrag spezifiziert ist, müssen keine entsprechenden Weisungsrechte vereinbart werden. Je besser also Dienstleister auf Grundlage eines klaren Auslagerungsvertrags handeln können, desto seltener erschweren ihnen besondere Weisungen einzelner Institute die Arbeit.

Bei wesentlichen Auslagerungen müssen im Vertrag Regelungen über die Möglichkeit einer Weiterverlagerung von Dienstleistungen an einen Dritten (Sub-Dienstleister) vereinbart werden. Denn auch bei Weiterverlagerungen muss sichergestellt sein, dass das Institut die bankaufsichtsrechtlichen Anforderungen weiterhin einhalten kann. Somit können das auslagernde Institut und der Dienstleister bereits im Auslagerungsvertrag vereinbaren, dass bestimmte Aktivitäten und Prozesse ohne explizite Zustimmung auf einen Dritten ausgelagert werden können, soweit sichergestellt wird, dass die bankaufsichtlichen Anforderungen erfüllt werden und im Einklang mit den vertraglichen Vereinbarungen des originären Auslagerungsvertrags stehen. Zudem muss bei Weiterverlagerungen eine Informationspflicht des Auslagerungsunternehmens gegenüber dem auslagernden Institut enthalten sein. In der Konsequenz bedeutet dies eine Erleichterung für den Dienstleister, da er nicht bei jeder beabsichtigten Weiterverlagerung auf Dritte mit sämtlichen Instituten Kontakt aufnehmen und deren Zustimmung einholen muss.

Für Cloud-Verträge gelten erweiterte vertragliche Anforderungen (z.B. Real-Time Monitoring) oder beim Hybrid-Cloud-Betrieb ist eine exakte Leistungsabgrenzung und -beschreibung erforderlich.

Besondere Herausforderungen für die Cloud



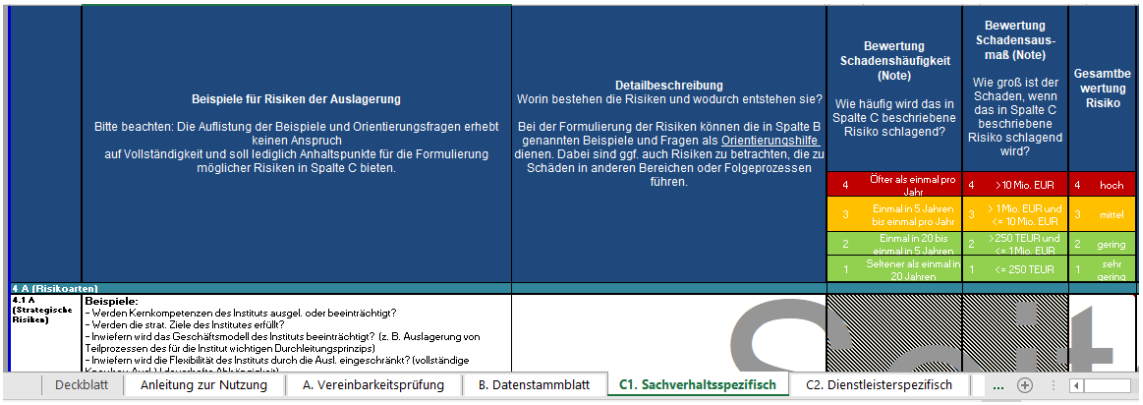
2.3.3 Risikoanalyse

Eine Risikoanalyse ist zunächst für jede neue Auslagerung auf der Grundlage einheitlicher institutsweiter Rahmenvorgaben vor Vertragsabschluss durchzuführen.

Eine erneute Risikoanalyse ist bei Änderungen der Auslagerungsdienstleistung sowie dann erforderlich, wenn dem auslagernden Institut Umstände bekannt werden, die darauf schließen lassen, dass sich die bei der Risikoanalyse verwendeten Risikofaktoren verändert haben (anlassbezogene Risikoanalyse). Praktische Beispiele hierzu sind: Gesellschaftsrechtliche Veränderungen beim Dienstleister, Veränderungen beim Dienstleistungsumfang, Bekanntwerden wesentlicher Feststellungen im Rahmen von Prüfungen beim Dienstleister etc.

Zudem ist die Risikoanalyse in regelmäßigen Zeitabständen zu erneuern, auch wenn kein Anlass besteht (regelmäßige Risikoanalyse). Ein Zeitraum von einem Jahr bei wesentlichen und von drei Jahren bei unwesentlichen Auslagerungen wird für angemessen erachtet.

Muster Risikoanalyse



	Beispiele für Risiken der Auslagerung Bitte beachten: Die Auflistung der Beispiele und Orientierungsfragen erhebt keinen Anspruch auf Vollständigkeit und soll lediglich Anhaltspunkte für die Formulierung möglicher Risiken in Spalte C bieten.	Detailbeschreibung Worin bestehen die Risiken und wodurch entstehen sie? Bei der Formulierung der Risiken können die in Spalte B genannten Beispiele und Fragen als Orientierungshilfe dienen. Dabei sind ggf. auch Risiken zu betrachten, die zu Schäden in anderen Bereichen oder Folgeprozessen führen.	Bewertung Schadenshäufigkeit (Note) Wie häufig wird das in Spalte C beschriebene Risiko schlagend?	Bewertung Schadensausmaß (Note) Wie groß ist der Schaden, wenn das in Spalte C beschriebene Risiko schlagend wird?	Gesamtbewertung Risiko
			4 Öfter als einmal pro Jahr	4 >10 Mio. EUR	4 hoch
			3 Einmal in 5 Jahren bis einmal pro Jahr	3 > 1Mio. EUR und <= 10 Mio. EUR	3 mittel
			2 Einmal in 20 bis einmal in 5 Jahren	2 >250 TEUR und <= 1Mio. EUR	2 gering
			1 Seltener als einmal in 20 Jahren	1 <= 250 TEUR	1 sehr gering
4 A (Risikoarten)					
4.1 A (Strategische Risiken)	**Beispiele:** - Werden Kernkompetenzen des Instituts ausgel. oder beeinträchtigt? - Werden die strat. Ziele des Institutes erfüllt? - Inwiefern wird das Geschäftsmodell des Instituts beeinträchtigt? (z. B. Auslagerung von Teilprozessen des für die Institut wichtigen Durchleitungsprinzips) - Inwiefern wird die Flexibilität des Instituts durch die Ausl. eingeschränkt? (vollständige				

Deckblatt | Anleitung zur Nutzung | A. Vereinbarkeitsprüfung | B. Datenstammblatt | C1. Sachverhaltsspezifisch | C2. Dienstleisterspezifisch | ...

Was sind die konkreten Schritte bei der Risikoanalyse:

Zunächst muss detailliert geprüft werden (mit Begründung), ob es sich um eine kritische oder wichtige Funktion handelt, die ausgelagert wird und ob überhaupt eine Auslagerung gemäß der Aufsicht und den institutseigenen Compliance-Regelungen möglich ist, die sogenannte „Vereinbarkeitsprüfung".

Für jeden Dienstleister ist eine „Geeignetheitsprüfung" bzw. Due Diligence durchzuführen. Hier wird u.a. großer Wert auf die Sicherheit und Zukunftsfähigkeit des Dienstleisters gelegt.

Anschließend muss eine umfangreiche Risikoeinwertung für jede einzelne Auslagerung vorgenommen werden. Hierbei ist u.a. die Auswirkung der Auslagerung und das damit verbundene Risiko auf das eigene IKS zu betrachten und zu bewerten.

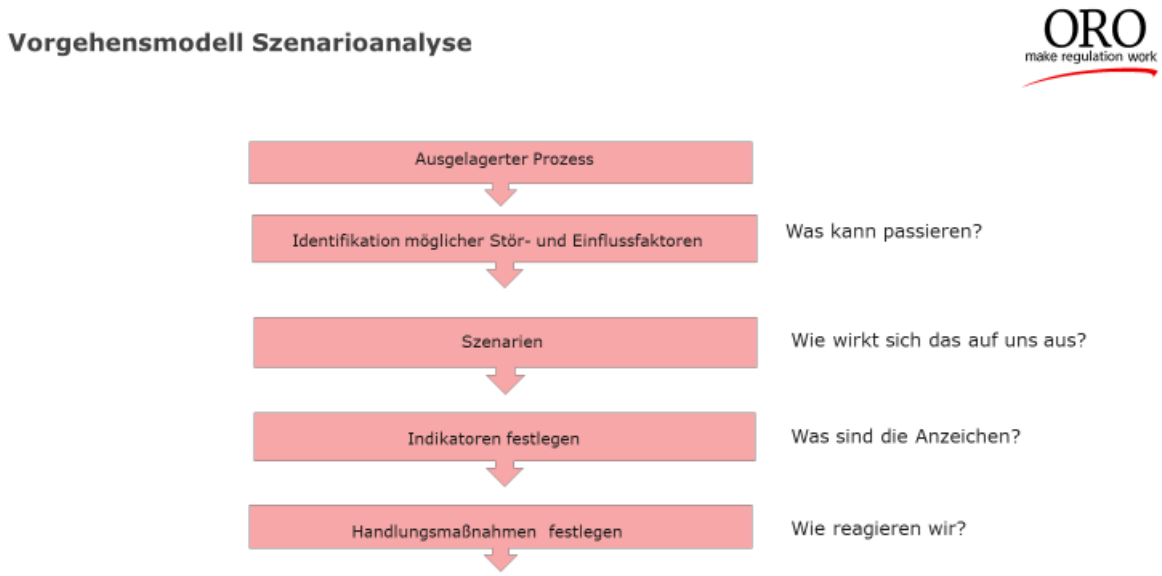
Bei der Risikoanalyse sind alle für das Institut relevanten Aspekte im Zusammenhang mit der Auslagerung zu berücksichtigen, so insbesondere Konzentrationsrisiken durch die Auslagerungen vieler wesentlicher Prozesse auf einen Dienstleister oder die Risiken aus Weiterverlagerungen.

Folgende Parameter sollten daher zur Bewertung des Risikos herangezogen werden:

- Kosten der Auslagerung (inklusive der Transaktionskosten)
- Auswirkungen der Auslagerung auf das Institut und insbesondere auf dessen IKS
- Komplexität des auszulagernden Prozesses, da mit zunehmender Komplexität i. d. R. auch das Risiko steigt
- Konsequenzen, bei Schlecht- oder Nicht-Leistung
- Aufwand zur Suche und Umlagerung der Prozesse auf alternative Dienstleister bzw. der Re-Integration von Aktivitäten und Prozessen
- Qualität der Dienstleistungen, wobei erst bei wiederholter Risikoanalyse bewertbar
- Wirtschaftliche und personelle Lage sowie Zukunftsfähigkeit (s. Due Diligence) des Auslagerungsunternehmens
- Weiterverlagerungen

Die Intensität der Risikoanalyse hängt von Art, Umfang, Komplexität und Risikogehalt der ausgelagerten Aktivitäten und Prozesse ab.

In Abhängigkeit von der Wesentlichkeit und Komplexität des ausgelagerten Prozesses, verlangt die Aufsicht künftig zusätzlich die Durchführung von Szenarioanalysen zur Bewertung und Ermittlung der Veränderung des operationellen Risikos.



2.3.4 Ausstiegszenarien

Für wesentliche Auslagerungen müssen im Fall einer erwarteten oder unerwarteten Beendigung der Auslagerung Maßnahmen für die Kontinuität und Qualität der Geschäftsprozesse getroffen werden. Für Fälle unbeabsichtigter oder unerwarteter Beendigung dieser Auslagerungen, die mit einer erheblichen Beeinträchtigung der Geschäftstätigkeit verbunden sein können, hat das Institut etwaige Handlungsoptionen auf ihre Durchführbarkeit zu prüfen.

Die Auswahl geeigneter Maßnahmen im auslagernden Unternehmen ist mit Blick auf die einer Beendigung zugrundeliegenden Ursachen vorzunehmen. Bei der beabsichtigten Beendigung eines Auslagerungsverhältnisses kommen Schlecht- oder Nichtleistung des Dienstleisters, eine nachteilige Kostenentwicklung oder eine strategische Neuausrichtung beim Institut in Frage. Aber auch der Dienstleister kann die Beendigung der Auslagerung anstreben. Ursächlich könnten Probleme mit der Auslagerungsvereinbarung, geänderte Kostenstrukturen oder mangelnde Mitwirkungspflichten sein. Hier ist ebenfalls davon auszugehen, dass das auslagernde Institut die Beendigung erwarten konnte. In beiden Fällen wird das Institut im Eigeninteresse rechtzeitig nach Ersatzlösungen suchen. Voraussetzung ist die Vereinbarung entsprechender Kündigungsrechte und angemessener Kündigungsfristen im Auslagerungsvertrag.

Für den Fall, dass die Auslagerungsbeziehung unbeabsichtigt bzw. unerwartet beendet wird, wie z. B. der plötzliche Ausfall des Dienstleisters infolge von technischen Problemen, helfen Kündigungsfristen nicht

weiter. Die Kontinuität und Qualität der Dienstleistung kann dann zumindest teilweise vorübergehend durch Notfallkonzepte sichergestellt werden. Dabei ist es von entscheidender Bedeutung, dass die Notfallpläne des Dienstleisters und die des auslagernden Instituts aufeinander abgestimmt sind.

Neben den abgestimmten Notfallplänen erwartet die Aufsicht die Nennung von weiteren Handlungsoptionen (z.B. konkrete Absichtserklärungen mit einem alternativen Dienstleister) und darüber hinaus auch eine Analyse, inwieweit diese praktisch umsetzbar sind.

Es empfiehlt sich, im Rahmen der Risikoanalyse die Qualität des Notfallmanagements des Dienstleisters zu beurteilen und die ausgelagerten Aktivitäten und Prozesse hinsichtlich ihrer Zeitkritikalität einzustufen. Auf Basis dieser Erkenntnisse kann das auslagernde Institut seine Überlegungen zu den geforderten Handlungsoptionen sammeln, bewerten und dokumentieren. Darüber hinaus sind Aktivitäten im Zusammenhang mit möglichen Handlungsoptionen im Rahmen der Dienstleistersteuerung zu überprüfen und zu verfolgen.

2.3.5 Notfallmanagement

Die Auslagerung von Geschäftsprozessen unter dem Blickwinkel der Notfallvorsorge, bedeutet nichts anderes, als dass die Anzahl der Risiken steigt, die außerhalb des eigenen, internen Einflussbereiches liegen. Damit verbunden ist ein Kontrollverlust. Zusätzlich steigen die Risiken für interne Geschäftsprozesse, wenn sie von diesen Dienstleistern abhängig sind. Um hier entgegenzuwirken, ist sowohl bei der Organisation und der Vertragsgestaltung neuer Auslagerungen oder Liefervereinbarungen, als auch bei bestehenden Auslagerungen in Bezug auf das Notfallmanagement etliches zu beachten. So ist sicherzustellen, dass die Anforderungen des eigenen Notfallmanagements an den (auszulagernden) Geschäftsprozess in den Verträgen entsprechend berücksichtigt werden. Der Dienstleister muss Wiederanlauf- und Wiederherstellungspläne für die ausgelagerten Prozesse erstellen. Vom Notfallmanagement des Instituts müssen diese auf ihre Funktionsfähigkeit überprüft werden. Bei wesentlichen Auslagerungen ist es darüber hinaus erforderlich, gemeinsame Notfall-Übungen durchzuführen.

Zusätzlich zu den gemeinsamen Übungen muss der Dienstleister seine Notfall-Fähigkeit insbesondere in Bezug auf die ausgelagerten Prozesse durch weitere regelmäßige Tests und Übungen nachweisen und dokumentieren. Die konkrete Zusammenarbeit in einem Notfall oder einer Krise ist ebenfalls zu dokumentieren, inklusive aller Rechte und Pflichten.

Das Institut selbst muss bei der Erstellung der Notfallpläne die Schnittstellen von internen zu ausgelagerten Prozessen genau definieren. Die Notfall-Prozeduren des Outsourcing-Dienstleisters müssen kompatibel mit denen des Instituts sein.

Der Nachweis der Notfall- und Krisenmanagement-Fähigkeit des Dienstleisters durch eine Zertifizierung oder eine andere unabhängige Prüfung ist möglich, doch muss das Institut genau darauf achten, ob seine ausgelagerten Geschäftsprozesse im Geltungsbereich der Zertifizierung auch enthalten sind.

2.3.6 Qualitätskontrolle/Reporting/KPI

Institute müssen die mit wesentlichen Auslagerungen verbundenen Risiken angemessen steuern und die ausgelagerten Aktivitäten auch regelmäßig überwachen. Dies ist in einem expliziten Auslagerungsbericht in das eigene Berichtswesen aufzunehmen. Es muss ausdrücklich darüber berichtet werden, ob die erbrachten Dienstleistungen der Auslagerungsunternehmen den vereinbarten Leistungen entsprechen (Service-Level/KPI). Es empfiehlt sich, je ausgelagertem Prozess ein Monitoring mit aussagekräftigen Kennzahlen einzurichten. Zusätzlich muss auch der Grad festgelegt werden, der für eine Schlechtleistung (noch) toleriert wird sowie ein entsprechender Maßnahmenkatalog.

Zu den Überwachungsmaßnahmen gehören auch die Analyse der Risikoberichte des Dienstleisters sowie eine Kontrolle der Revisionsberichte bzw. vorliegender Zertifizierungen nach gängigen Standards (BSI, ISO, IDW oder ISAE).

Die Überwachung der Dienstleistung muss in jedem Fall nachvollziehbar dokumentiert werden. Konkret bietet es sich an, die Kontrolle aus verschiedenen Perspektiven wahrzunehmen:

1. Die organisatorische Perspektive (Qualität der einzelnen Leistungserbringung).
2. Die wirtschaftliche Perspektive (Budgetauslastung).
3. Die aufsichtsrechtliche Perspektive (Adressenausfallrisiko, Abhängigkeitsrisiko, Reputationsrisiko, Weiterverlagerungen, Angemessenheit des Internen Kontrollsystems, operationelle Risiken beim Dienstleister).

All diese Perspektiven müssen in einer regelmäßigen, zusammenfassenden Beurteilung berücksichtigt werden.

2.3.7 Berichtswesen

Neben den regelmäßigen Qualitäts- und Kontrollberichten muss das Auslagerungsmanagement auch mindestens einmal jährlich einen umfassenden Bericht über seine Aktivitäten aufstellen. Die Erwartung der Aufsicht geht jedoch eher von Quartalsberichten aus. Der Bericht ist der Geschäftsleitung zur

Verfügung zu stellen und soll u.a. Aussagen über die Vertragskonformität der Dienstleistung, die Angemessenheit der Steuerung und Überwachung der Dienstleistung sowie ggf. den Bedarf weiterer risikominimierender Maßnahmen enthalten.

Muster Jahresbericht Dienstleistungsmanagement

Berichtsinhalt	Erläuterung
Wesentliche Auslagerungen	▪ Portfolio der wesentlichen Auslagerungen ▪ Messung der jeweiligen Dienstleistungsqualität (Bezug auf die Service -Level-Agreements (SLA), alternativ KPI -Überwachung ▪ Einhaltung der vertraglichen Vereinbarungen ▪ Vorhandensein der Revisionsfunktion (MaRisk) im Auslagerungsunternehmen ▪ Aktuelle Risikoanalyse
Nicht wesentliche Auslagerungen	▪ Portfolio der nicht wesentlichen Auslagerungen ▪ Messung der jeweiligen Dienstleistungsqualität (Bezug auf die Service -Level-Agreements (SLA), alternativ KPI -Überwachung ▪ Einhaltung der vertraglichen Vereinbarungen ▪ Vorhandensein der Revisionsfunktion (MaRisk) im Auslagerungsunternehmen ▪ Aktuelle Risikoanalyse (jährlicher Turnus empfohlen)
Sonstiger Fremdbezug von Leistungen	▪ Portfolio des sonstigen Fremdbezugs von Leistungen ▪ Messung der jeweiligen Dienstleistungsqualität (Bezug auf die Service -Level-Agreements (SLA), alternativ KPI -Überwachung – gehört zu den Überwachungspflichten nach § 25a KWG ▪ Einhaltung der vertraglichen Vereinbarungen
Sonstiger Fremdbezug von IT-Dienstleistungen	▪ Portfolio des sonstigen Fremdbezugs von IT-Dienstleistungen ▪ Messung der jeweiligen Dienstleistungsqualität (Bezug auf die Service -Level-Agreements (SLA), alternativ KPI -Überwachung – gehört zu den Überwachungspflichten nach § 25a KWG ▪ Einhaltung der vertraglichen Vereinbarungen ▪ Aktuelle Risikoanalyse (Muss)
Sonstige institutstypische Dienstleistungen	▪ Portfolio der sonstigen institutstypischen Dienstleistungen ▪ Messung der jeweiligen Dienstleistungsqualität (Bezug auf die Service -Level-Agreements (SLA), alternativ KPI -Überwachung – gehört zu den Überwachungspflichten nach § 25a KWG ▪ Einhaltung der vertraglichen Vereinbarungen

3. Ihr Nutzen - unser Angebot

ORO verfügt über ein vollumfängliches, aufsichts - und prüfungsbewährtes Best Practice Vorgehensmodell für das Auslagerungsmanagement. Dieses hilft Ihnen, den vielfältigen Risiken des Auslagerungsmanagements strukturiert und effizient entgegenzuwirken und dabei komplexen aufsichtsrechtlichen Anforderungen gerecht zu werden, ohne dabei die wirtschaftliche Perspektive außer Acht zu lassen.

ORO unterstützt Sie mit drei wesentlichen Angeboten:

_ Bestandscheck

_ Umsetzungsberatung

_ Outsourcing einzelner Aufgaben des ZAM oder Komplettauslagerung

ORO Unterstützungsangebote

_ Geprüfte Mustervorlagen: Auslagerungsregister, Risikoanalyse etc.
_ Einmaliger Bestands-Check
_ Einmaliger Bestands-Check + Umsetzungsberatung
_ Einmaliger Bestands-Check+ Insourcing des Auslagerungsmanagement

3.1 Bestands-Check

Gemeinsam mit unserem Mandanten wird eine kompakte Bestandsanalyse der institutsspezifischen Situation (Art, Umfang, Komplexität, Risikogehalt der Geschäfte) durchgeführt. Welche konkreten Anforderungen wirken sich wie auf das Institut aus? Die Auswirkungen können dabei abhängig vom Geschäftsmodell, der Größe oder Komplexität der Bank sein. Welche Prozesse sind essentiell für das Fortbestehen und den Erfolg? Wie sind diese organisiert und in welchen Bereichen ggf. durch Externe unterstützt?

Gestartet wird immer mit einem kompakten Outsourcing Bestands-Check. Ziel ist es, möglichst schnell einen Gesamtüberblick über die Ist-Situation des Auslagerungsmanagements, die größten Risikopotentiale und die wichtigsten To-Do´s zu bekommen.

Die Organisation des Auslagerungsmanagements wird aufbau- und ablauforganisatorisch betrachtet. Gibt es einen hinreichenden qualifizierten zentralen Auslagerungsbeauftragten, der idealerweise durch ein Team des zentralen Auslagerungsmanagements unterstützt wird? Stehen genug qualitative und quantitative Ressourcen zur Verfügung? Sind die Governance-Regelungen vollständig und dabei hinreichend konkret genug?

Die vorliegenden Risikoanalysen werden im Rahmen einer ersten Standortbestimmung auf Vollständigkeit und Inhalt analysiert. Dabei erfolgt ein Scoring punktueller Analysen hinsichtlich der folgenden Kriterien:

_Risiken der Auslagerung

_Eignung des Auslagerungsunternehmens

_Risiken aus der Vertragsgestaltung

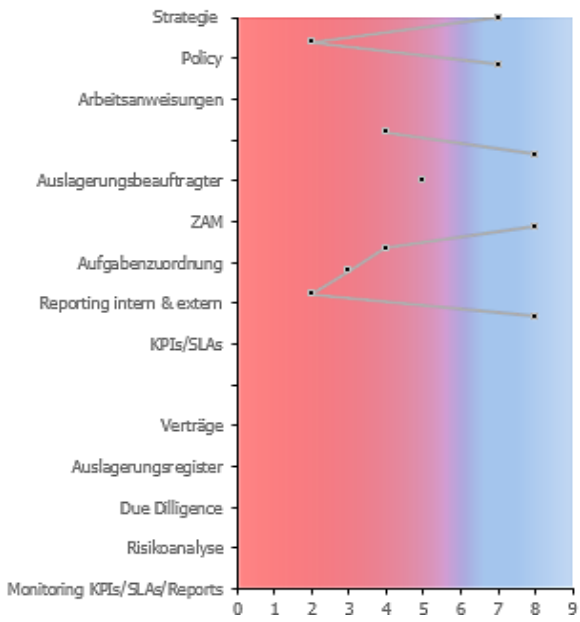
Aus den Verträgen sollten sich auch das mit dem Dienstleister vereinbarte Qualitätslevel und die einzuhaltenden KPIs/SLAs ergeben. Wie wird dieses Monitoring in der Praxis erfüllt? Wer kontrolliert, wann und wie oft die Dienstleistungsqualität?

Ein weiterer wichtiger Baustein sind die Exit- bzw. die Notfallpläne. Welche Vorkehrungen sind bei Beendigung der Dienstleistung getroffen bzw. wie sind die Notfallpläne gestaltet? Sind diese abgestimmt mit denen des Dienstleisters? Werden Tests durchgeführt?

Das Ergebnis des kompakten Bestands-Checks wird in Form einer übersichtlichen Risikoverortung zusammengefasst.

Risikoverortung

9 = Beste Bewertung	
1 = Schlechteste Bewertung	
Governance	
Strategie	7
Policy	2
Arbeitsanweisungen	7
Organisation & Steuerung	
Auslagerungsbeauftragter	4
ZAM	8
Aufgabenzuordnung	6
Reporting intern & extern	5
KPIs/SLAs	5
Operationalisierung & Prozesse	
Verträge	8
Auslagerungsregister	4
Due Dilligence	3
Risikoanalyse	2
Monitoring KPIs/SLAs/Reports	8



3.2 Umsetzungsberatung

Aufbauend auf dem Bestands-Check werden in Workshops die Handlungsfelder analysiert und unter Einbindung der beteiligten Unternehmenseinheiten wird ein einheitliches Vorgehen erarbeitet.

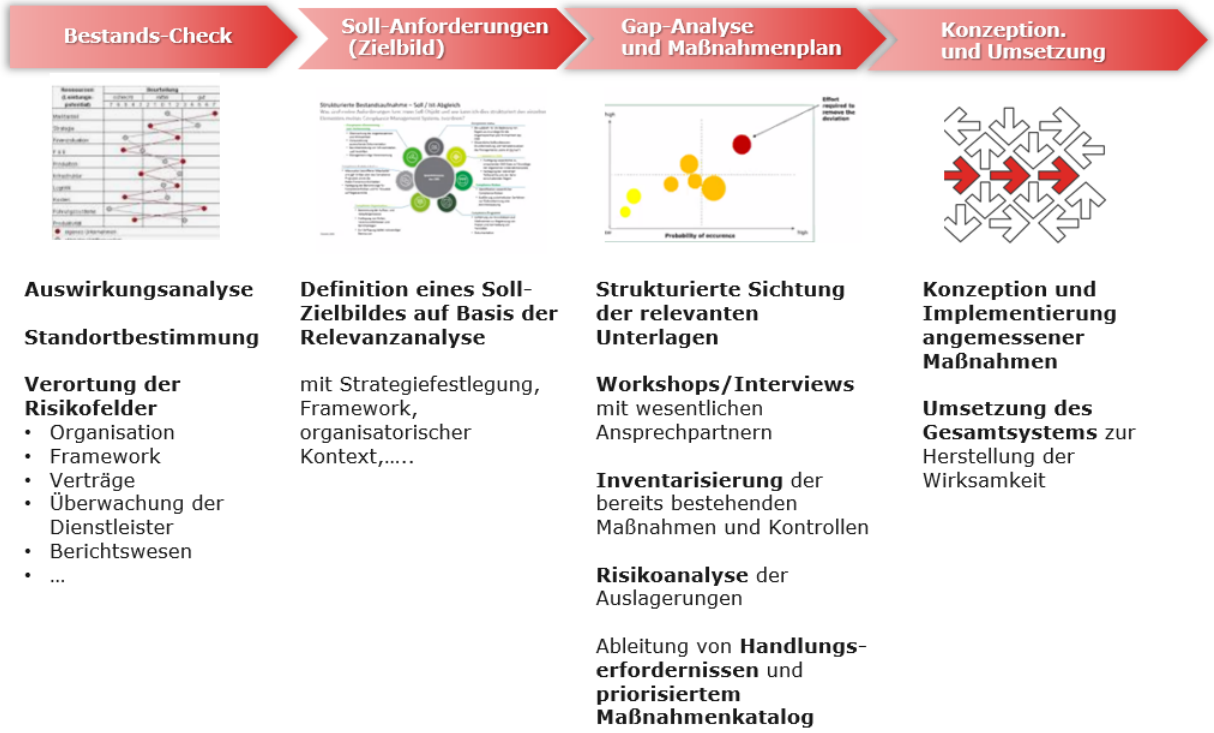
Dabei stehen neben den akuten Handlungsfeldern folgende Punkte im Vordergrund:

- Erarbeitung einer einheitlichen Risikoanalyse
- Vertragsmanagement inkl. Service-Level-Agreements
- Implementierung effizienter Steuerungs- und Überwachungsprozesse
- Unterstützung bei der jährlichen Berichterstattung

Nach erfolgreicher Projektdurchführung wird eine prüfungssichere Dienstleistersteuerung implementiert bzw. weiterentwickelt. Eine MaRisk- und BAIT-konforme Methodik wird erarbeitet und anhand von einheitlichen Bewertungskriterien und Prozessen wirtschaftlich ausgestaltet.

Der konkrete Beratungsumfang ist dabei von der individuellen Situation des Instituts und der Risikoverortung abhängig. Er kann erst nach dem Bestandscheck seriös festgelegt werden und wird in einem individuellen Beratungsangebot konkretisiert.

Vorgehensmodell Bestands-Check & Beratung



3.3 Outsourcing

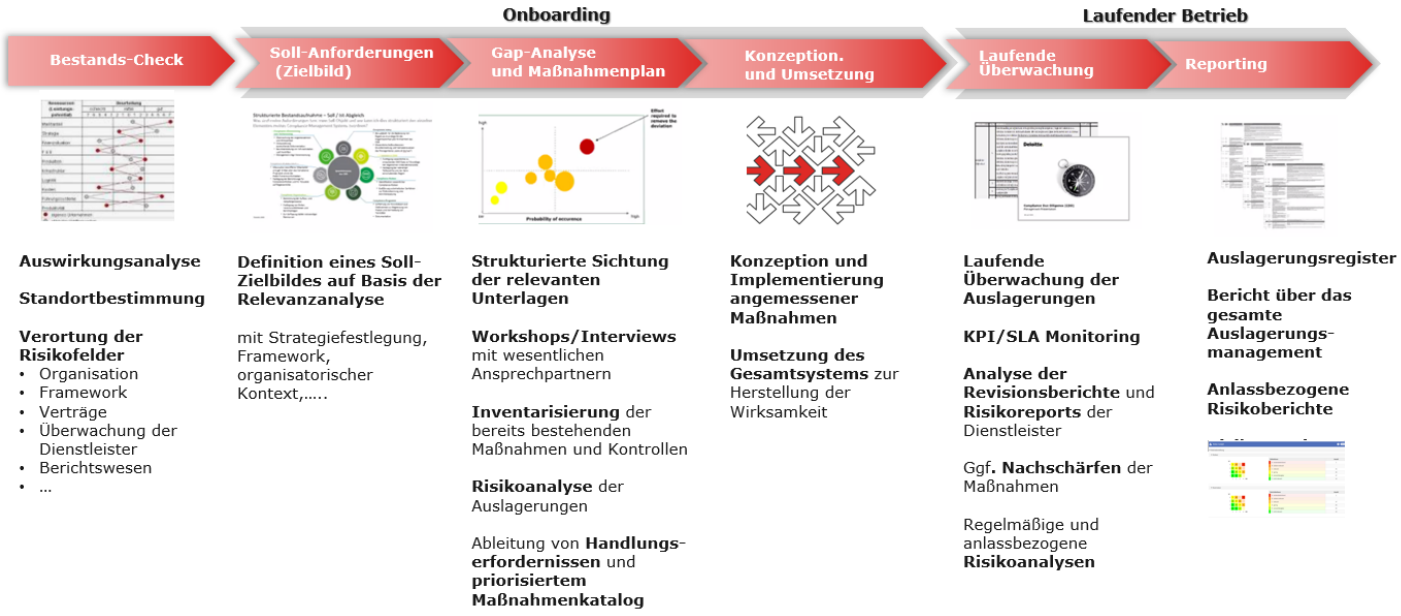
Basierend auf dem Bestands-Check können sich Organisationen entscheiden, direkt die Unterstützungsleistung/das ZAM auszulagern. Eine Auslagerung der Funktion des zentralen Auslagerungsbeauftragten ist gesetzlich nicht möglich, jedoch bietet ORO Services das Insourcing weitgehender operativer Tätigkeiten des ZAM sowie wesentliche Unterstützungsarbeiten für den Auslagerungsbeauftragten an. Zahlreiche aufsichts- und prüfungserprobte Methoden und Best-Practice Ansätze werden eingesetzt. Näheres ist in unserer Schnittstellen-Matrix ersichtlich.

Nach dem Bestands-Check mit Risikoverortung wird das Insourcing der Prozesse durch ein "Onboarding-Projekt" vorbereitet. Ziel ist zum einen eine rasche Risikominimierung durch die Erfüllung der regulatorischen Anforderungen, zum anderen die Implementierung unserer bewährten Best-Practice Prozesse und Standards.

Hierzu nutzen wir ein ebenfalls in der Praxis erprobtes "Auslagerungs-Management-Tool". Das Tool ist webbasiert und ermöglicht uns, die Administration und die operative Umsetzung mit Aufgabenworkflow oder Zustimmungsdokumenten zentral zu steuern. Dem Mandanten wird ebenfalls ein Zugriff eingerichtet, Aufgaben können direkt im Tool bearbeitet werden.

Das Tool dokumentiert die Risikosituation und die offenen To-Do`s in einem übersichtlichen Cockpit.

Vorgehensmodell Insourcing



4. Ihr Partner

Outsourced Regulatory Office
für Finanzunternehmen

ORO Services GmbH („Outsourced Regulatory Office") wurde mit dem Ziel gegründet, mit einem neuen innovativen Ansatz Banken bei der Bewältigung regulatorischer Anforderungen zu unterstützen.

Das Kernprodukt von ORO-Services GmbH ist **Regupedia®, das Informationsportal für Bankenregulierung** (www.regupedia.de), das tagesaktuelle News, Regularien, generische Auswirkungsanalysen, Terminübersichten sowie einen eigenen Blog beinhaltet. Das kostenpflichtige Portal wird um weitere ORO-Dienstleistungen im Bereich der Umsetzung regulatorischer Vorgaben und der Compliance ergänzt.

ORO verfügt über ein eigenes Expertenteam mit langjähriger Erfahrung im Risikomanagement, im Bereich Compliance, in der Umsetzung regulatorischer Anforderungen sowie im Management komplexer Großprojekte.

Zur Ergänzung seiner Expertise arbeitet ORO eng mit **Severn Consultancy GmbH** (www.severn.de) in Frankfurt am Main zusammen. Severn ist ein auf Finanzdienstleister spezialisiertes Beratungshaus, das seine weltweit operierenden Mandanten aktiv bei der Durchführung unternehmenskritischer Projekte, immer unter Berücksichtigung aktueller Marktanforderungen und aufsichtsrechtlicher Rahmenbedingungen, unterstützt.

Ansprechpartner:

Verena Siemes | Geschäftsführerin

ORO Services GmbH
Hansa Haus, Berner Straße 74
60437 Frankfurt am Main
T +49 (0)69 / 950 900-0
F +49 (0)69 / 950 900-50
verena.siemes@oro-services.de
www.regupedia.de