

# Auslagerung nach MaRisk

Zitiervorschlag:

*Autor* in: Auslagerung nach MaRisk, S. XX.

Download der Abbildungen unter [www.FC-Heidelberg.de](http://www.FC-Heidelberg.de)  
im persönlichen Benutzerbereich (Menüpunkt Mein FCH): **Zugangscod**e **h4Co2**

ISBN: 978-3-95725-038-4  
© 2018 Finanz Colloquium Heidelberg GmbH  
Im Bosseldorn 30, 69126 Heidelberg  
[www.FC-Heidelberg.de](http://www.FC-Heidelberg.de)  
[info@FC-Heidelberg.de](mailto:info@FC-Heidelberg.de)  
Titelfoto: Silberberg GmbH Montafon  
Satz: Finanz Colloquium Heidelberg  
Druck: Strauss GmbH, Mörlenbach

# Auslagerung nach MaRisk

**Gisbert Beckmann**

Geschäftsführer

VR FinanzDienstLeistung GmbH

**Martin Daumann**

Rechtsanwalt, Head of Compliance

Degussa Bank AG

**Sarah Horn**

Rechtsanwältin, Prokuristin

Audit GmbH Karlsruhe Stuttgart Wirtschaftsprüfungsgesellschaft

**Tanja Thieking**

Leiterin Interne Revision

Kreissparkasse Tübingen

A. Definition, Zulässigkeit und Wesentlichkeit von Auslagerungen und die Erstellung einer Risikoanalyse ( <i>Daumann</i> )	7
I. Definition der Auslagerung (Checkliste & Detail Software)	7
II. Zulässigkeit von Auslagerungen (Checkliste)	8
III. Einstufung Wesentlichkeit	8
1. Allgemeine Erläuterung	8
2. Übersicht der möglichen Auslagerungen und deren Einstufung zur Wesentlichkeit	8
IV. Erstellung einer Risikoanalyse AT 9 Tz. 2 i. V. m. § 25b KWG	9
1. Allgemeine Aspekte	9
2. Risikoparameter	9
3. Bearbeitungshilfe zur Erstellung einer Risikoanalyse	10
4. Zeitraum zur Erstellung einer Risikoanalyse	10
B. Anforderungen an den Auslagerungsvertrag ( <i>Beckmann</i> )	15
I. Pflichtangaben	16
1. Vertragsgegenstand und Leistungspflichten der Auftragnehmerin	16
a) Grundlagen	16
b) Hauptleistungspflichten der Auftragnehmerin	17
c) Leistungsscheine	17
d) Änderungen der Leistungen	20
e) Art und Weise der Leistungserbringung	20
f) Ort der Leistungserbringung	21
g) Informationspflichten	22
h) Reporting	22
2. Steuerung und Kontrolle des ausgelagerten Bereiches	23
a) Vorliegen der erforderlichen Erlaubnisse	23
b) Steuerung und Kontrolle des ausgelagerten Bereichs	23
c) Leistungs- und Qualitätsstandards	29
d) Weiterverlagerung	29
e) Business Continuity Management	30

3. Weitere rechtliche Bestimmungen	33
a) Datenschutz	33
b) Compliance	34
c) Verhinderung von Geldwäsche, Terrorismusfinanzierung und sonstigen strafbaren Handlungen	35
4. Informationssicherheitsmanagement (ISMS)	36
5. Grundsätze und Richtlinien zu Buchführung und Datenverarbeitung	37
6. Erweitertes IDW PS 951-Zertifikat	38
II. Notfallkonzept bei fristgerechter Beendigung	40
1. Ordentliche Kündigung des Vertrages und von Leistungen	40
2. Rechtsfolgen der Beendigung	41
a) Fortgeltungsfiktion	41
b) Rückgabepflichten	42
c) Vertragsmigration	42
d) Verfahrensplan	42
e) Vergütung für den Überleitungsaufwand	43
f) Fortwirkung von Rechten und Pflichten	43
III. Notfallkonzept bei fristloser Beendigung	44
C. Anforderungen an ausgelagerte Bereiche und Steuerung der mit der Auslagerung verbundenen Risiken	45
I. Entwicklung einer Strategie	45
1. Erfordernis einer Strategie	45
2. Strategieprozess	46
a) Plan – Strategieerstellung	47
b) Do – Strategieumsetzung	49
c) Check – Beurteilung der Strategieeinhaltung	50
d) Act – Strategieanpassung	51
II. Zuständigkeiten	51
1. Geschäftsleitung	51
2. Fachverantwortlicher	52
a) neue Fremdbezugsvorhaben	52

b) laufende Steuerung und Überwachung	53
3. zentrales Auslagerungsmanagement	54
4. weitere Beauftragtenfunktionen (zweite Verteidigungslinie)	56
5. Interne Revision	57
III. Betriebswirtschaftliche Kosten-Nutzen-Analyse	57
1. Quantitative Beurteilung	58
2. Qualitative Beurteilung	58
IV. Risikoanalyse und Steuerung	60
1. Grundsätzliche Sichtweise	60
2. Risikoanalyse als Basis	61
a) Risikoanalyse als Entscheidungsgrundlage	61
b) Ableitung der Wesentlichkeit aus der Risikoanalyse	62
c) Risikoanalyse als Grundlage der Kontrollhandlungen	63
3. Risikoüberwachung	64
4. Leistungsüberwachung	68
5. Kostenüberwachung	69
6. Bericht an die Geschäftsleitung	69
V. Regelmäßige Überprüfung der Auslagerung	70
VI. Beispiel einer Beschlussvorlage	71
D. Prüfung von Auslagerungen aus Sicht der Revision ( <i>Thiecking</i> )	73
I. Einleitung	73
II. Prüfungsfelder	73
1. Prüfungsplanung	74
2. Auslagerung als Prüfungsobjekt	74
3. Prüfung im Rahmen von neuen Auslagerungen	78
4. Prüfung im Rahmen von bestehenden Auslagerungen	82
5. Prüfung bei Beendigung von Auslagerungen	83

# Auslagerung nach MaRisk

## A. Definition, Zulässigkeit und Wesentlichkeit von Auslagerungen und die Erstellung einer Risikoanalyse

### Überblick

Arbeitsteilung ist seit Langem ein wichtiger Treiber des wirtschaftlichen Wachstums und damit auch des gesellschaftlichen Wohlstands unseres Landes. Die Auslagerung ist letztlich nur eine spezielle Form der Arbeitsteilung, die gerade bei Banken und Finanzdienstleistern eine besonders wichtige Rolle spielt, weshalb der deutsche Gesetzgeber seit 1998 in § 25a Abs. 2 KWG und Nachfolgeregelungen den Rahmen für Auslagerungsaktivitäten abgesteckt hat. Die Auslagerung betraf zunächst vor allem die IT, den Zahlungsverkehr oder die Wertpapierabwicklung.<sup>1</sup>

Angesichts des gestiegenen Kostendrucks im Gefolge von Niedrigzins und Digitalisierung verwundert es daher nicht, dass die Banken vermehrt die Auslagerung entdecken. Hierauf hat die Aufsicht gerade wiederum (auch aufgrund der zum Teil von ihr wahrgenommenen zweifelhaften Qualität einiger Dienstleister) mit umfassender Verschärfung der Vorgaben für Auslagerungen in den MaRisk 6.0 reagiert. Diese bilden einen Schwerpunkt der Novellierung, weshalb die nachfolgenden Ausführungen

entsprechend Lösungsansätze und Muster für die Umsetzung dieser umfassenden Verschärfungen beinhalten.

### I. Definition der Auslagerung (Checkliste & Detail Software)

#### **AUSLAGERUNG? Liegt eine solche vor?**

- a. Eine andere Firma/Unternehmen?
- b. Beauftragung mit Aktivitäten/Prozessen bzgl. Bankgeschäften/Finanzdienstleistungen, sonst. Institutsspezifische Dienstleistungen?
- c. Kein sonstiger Fremdbezug?  
(Auslagerungstatbestand Software: Bei Software zur Risikosteuerung gelten die Aspekte:
  - „Bezug von Software“,
  - „Unterstützungsleistungen hierzu“ und ggf.
  - „Betrieb der Software durch Dritte“,

**nun als Auslagerung.** Nur Software, die nicht zur Risikosteuerung eingesetzt wird, gilt als Fremdbezug)

<sup>1</sup> Vgl. Hannemann/Schneider/Weigl, Mindestanforderungen an das Risikomanagement (MaRisk), 4. Auflage 2013, 543 f.

## II. Zulässigkeit von Auslagerungen (Checkliste)

Darf diese Tätigkeit ausgelagert werden?

- a. Keine Beeinträchtigung der Ordnungsmäßigkeit der Geschäftsorganisation
- b. Keine Leitungsdelegation, also
  - Unternehmensplanung, -kontrolle, -koordination
  - Besetzung von Führungskräften
  - Strategischen Entscheidungen
  - Zwingende Aufgaben (z. B. Gesetz)

## III. Einstufung Wesentlichkeit

### 1. Allgemeine Erläuterung

Aufgrund des Proportionalitätsgrundsatzes unterliegen Auslagerungen nur dann den besonderen Anforderungen des § 25b KWG, wenn es sich um „wesentliche Auslagerungen“ von Aktivitäten und Prozessen handelt. Die Beurteilung der Wesentlichkeit hat das Institut selbst auf Grundlage einer standardisierten und einheitlichen Risikoanalyse durchzuführen. Die Intensität der Analyse hängt von Art, Umfang, Komplexität, und Risikogehalt der ausgelagerten Aktivitäten und Prozesse ab. Daraus folgt, dass bei Auslagerungen **von erheblicher Tragweite** eine entsprechend intensive Prüfung vorzunehmen ist und Verallgemeinerungen nur schwer möglich sind.

Im Folgenden wird unter IV. Risikoanalyse die Frage der Wesentlichkeit anhand ausgewählter gängiger Aspekte im Rahmen der allgemeinen Risikoanalyse behandelt. Zum Teil wird hierfür eine separate Prüfung Teil 1 und Teil 2 vorgenommen.

### 2. Übersicht der möglichen Auslagerungen und deren Einstufung zur Wesentlichkeit

Ein umfassender Überblick über alle möglichen Auslagerungen und deren Einstufung der Wesentlichkeit würde den Rahmen dieses Buches sprengen. Zur Orientierung jedoch zwei Hinweise:

Mit Integration der Auslagerungsregelungen in die MaRisk 2007 sind die noch in Rundschreiben 11/2001 (aufgehoben) aufgeführten Beispiele unwesentlicher Bereiche entfallen, können jedoch der Orientierung dienen

- Inkassowesen,
- Geldautomatenversorgung,
- Wartung technischer Geräte (auch EDV) → Achtung nun ggf. „Sonstiger Fremdbezug“,

allgemeine Service- und Unterstützungsleistungen (wie z. B. Kantinen, Reinigungsdienst, Wachschatz, Betriebsarzt, Baudienst, Brandschutz usw.),

- reine Beratungsleistungen, insbesondere in Rechts- und Steuerangelegenheiten

auch dann, wenn sie nicht auf Einzelaspekte bzw. -projekte beschränkt sind. Die bislang umfassendste Einschätzung findet sich im Fachbuch „Outsourcing in Genossenschaftsbanken: Ein Leitfaden aus betriebswirtschaftlicher und rechtlicher Sicht“ als Ergebnis des BVR Arbeitskreises Outsourcing ISBN: 3871511730, 9783871511738 – allerdings aus dem Jahre 2015. Eine Anpassung auf die speziellen Erfordernisse der MaRisk 6.0 steht aus, bietet jedoch noch immer wertvolle Orientierung.

## IV. Erstellung einer Risikoanalyse AT 9 Tz. 2 i. V. m. § 25b KWG

*„Das Institut muss auf der Grundlage einer Risikoanalyse eigenverantwortlich festlegen, welche Auslagerungen von Aktivitäten und Prozessen unter Risikogesichtspunkten wesentlich sind (wesentliche Auslagerungen). Diese ist auf der Grundlage von institutsweit bzw. gruppenweit einheitlichen Rahmenvorgaben sowohl regelmäßig als auch anlassbezogen durchzuführen. Die maßgeblichen Organisationseinheiten sind bei der Erstellung der Risikoanalyse einzubeziehen. Im Rahmen ihrer Aufgaben ist auch die Interne Revision zu beteiligen.“*

### 1. Allgemeine Aspekte

Dreh- und Angelpunkt der Auslagerung ist die Risikoanalyse. Arbeitet man hier von Anfang an systematisch, akribisch und dokumentiert, so macht sich dies in der Folgezeit doppelt und dreifach bezahlt: Man kann z. B. die

- in den MaRisk vorgesehenen Erleichterungen nutzen
- schon erhobene Informationen in der Dienstleistersteuerung nutzen
- Argumentationen ggü. Prüfern umfassend hierauf stützen
- drohende Haftung des Vorstandes souverän abwenden.

Angesichts dieser Vorteile und dem gestiegenen Interesse der Aufsicht an dem Thema Auslagerung (Stichwort ein Schwerpunkt der Novellierung) dürfte der Anwendungsbereich für in

der Vergangenheit teilweise gerne eingesetzte „Instant“- oder „One-Pager“-Analysen künftig sehr überschaubar sein.

### 2. Risikoparameter<sup>2</sup>

Es werden in der Literatur einige gängige Risikoparameter zur Bewertung des auslagernden Unternehmens (Outsourcer) und des Auslagerungsunternehmens (Insourcer) besprochen:<sup>3</sup>

- die Kosten der Auslagerung (unter Berücksichtigung von Transaktionskosten),
- die Auswirkungen der Outsourcing-Maßnahme auf das auslagernde Institut,
- die Komplexität des Auslagerungsgegenstandes, da mit der Komplexität i. d. R. auch das Risiko der Auslagerungsmaßnahme steigt,
- die möglichen Konsequenzen, sofern das Auslagerungsunternehmen schlecht oder gar nicht leistet,
- der (Zeit-)Aufwand, der bei der Suche geeigneter Ersatzkandidaten bzw. der ReIntegration von Aktivitäten und Prozessen erforderlich wird,
- die Qualität der Dienstleistungen eines potenziellen Kandidaten (inkl. Supportfunktionen), wobei üblicherweise eine Betrachtung über einen längeren Zeitraum angestellt wird, damit sich das auslagernde Institut einen nachhaltigen Eindruck verschaffen kann,
- die wirtschaftliche Situation eines potenziellen Kandidaten sowie sein gesellschaftsrechtlicher und regulatorischer Status, wobei auch von Bedeutung ist, durch wen das Auslagerungsunternehmen beauf-

<sup>2</sup> Zur Umsetzung des Themas „institutsweite bzw. gruppenweit einheitliche Kriterien“ wie auch jeweils generell zum Thema MaRisk 6.0 sind im Muster diverse Passagen zur Umsetzung und Operationalisierung eingearbeitet. Neuerungen aufgrund der Novellierung sind in der Downloadvariante farblich hervorgehoben.

<sup>3</sup> Hannemann/Schneider/Weigl, Mindestanforderungen an das Risikomanagement, S. 558, 559.

- sichtigt wird (EWR, Drittstaat mit vergleichbarem Aufsichtsregime, sonstiger Drittstaat),
- die quantitative und qualitative Personalausstattung, wobei insbesondere für komplexe Auslagerungsmaßnahmen vorhandenes Spezial-Know-how eine wichtige Rolle spielt,
  - die Kapazitäten und die technische Leistungsfähigkeit eines potenziellen Kandidaten, vorhandene Sicherheitsmaßnahmen sowie die Kompatibilität der IT-Systeme bzw. passende IT-Schnittstellen,
  - der Ort der Leistungserbringung und die dortigen Gegebenheiten (z. B. Infrastruktur, Kultur, politisches System),
  - die Reputation eines potenziellen Kandidaten, seine Unternehmenskultur und sein Geschäftsmodell sowie mögliche Abhängigkeiten von weiteren Dienstleistern (Subunternehmen),
  - Vorkehrungen, die zu einer Risikominderung der Auslagerungsmaßnahme beitragen können, wie bspw. die Existenz eines wirksamen gruppenweiten Risikomanagements bei gruppeninternen Auslagerungen.

Letztlich muss jedes Institut einheitliche Standards für Risiko- und Wesentlichkeitsanalyse festlegen und in ein einheitliches Formular/Prozesse für das Haus gießen.

### 3. Bearbeitungshilfe zur Erstellung einer Risikoanalyse

Die nachfolgende Muster-Auslagerungs-Risikoanalyse gem. MaRisk At 9.2 ist am Beispiel der Auslagerung der Funktion der MaRisk-Compliance gem. 4.4.2 MaRisk (nur noch für kleine Banken zulässig) befüllt. In dem Muster sind möglichst viele Situationen/Erkenntnisse beispielhaft dargestellt. Eine solche „Ballung“ ist in

der Realität natürlich hochgradig unwahrscheinlich. Zugleich ist das Muster **nicht abschließend**. Vor diesem Hintergrund ist das Muster zu lesen und natürlich den Gegebenheiten und Besonderheiten (insbesondere der jeweiligen Auslagerung) des Hauses **anzupassen**.

Im nachfolgenden Beispiel mittels Scoring-Formulars wurde eine Kombination aus Risiko- und Wesentlichkeitsanalyse gewählt, bei der bestimmte Angaben aus der Risikoanalyse (Reifegrad) zugleich zur Klärung der Frage der Wesentlichkeit (Wesentlichkeit) genutzt werden. Dies ist jeweils durch Pfeile ➡ kenntlich gemacht.

Zunächst das Formular im Überblick, dann im Detail. Die einzelnen Score-Werte für Reifegrad und Wesentlichkeit sind im Einzelnen und gesamt (Stichwort Schwellenwerte) natürlich exemplarisch und vom Institut festzulegen. Sodann folgt das Beispiel.

### 4. Zeitraum zur Erstellung einer Risikoanalyse

Das Institut muss auf der Grundlage einer Risikoanalyse eigenverantwortlich festlegen, welche Auslagerungen von Aktivitäten und Prozessen unter Risikogesichtspunkten wesentlich sind (wesentliche Auslagerungen). Diese ist auf der Grundlage von institutsweit bzw. gruppenweit einheitlichen Rahmenvorgaben sowohl **regelmäßig** als auch **anlassbezogen** durchzuführen.

Ein üblicher Zeitraum für die Erstellung einer regulären Risikoanalyse ist oft in der Praxis wie folgt definiert: „Regelmäßig, zumindest jedoch jährlich“. Eine Altregelung ist in den MaRisk nicht vorgesehen, so dass alle Auslagerungen entsprechend zu bewerten sind.

Sofern pauschal eine vierteljährliche Risikoanalyse verlangt wird, ist ein Risiko-Aufwandsangemessenes Vorgehen entgegenzuhalten: Es erfolgt laufend eine Dienstleistungssteuerung (MaRisk AT 9.7), so dass bei Auffällig-

keiten ad hoc eine anlassbezogene Risikoanalyse (MaRisk AT9.2) durchgeführt werden kann.

Eine Zyklizität von mindestens „jährlich“ erscheint daher angemessen.

Formular 9.2 Risikoanalyse Auslagerung ÜBERBLICK

instituts- / Gruppenweite Risikoanalyse: Wesentlichkeit & Reifegrad einer Auslagerung (gemäß MaRisk AT 9 Tz. 2)			
	Reifegrad	Wesentlichkeit	
<b>A. Auslagerungsgründe und -vorteile*</b>	JA (1) / NEIN (0)	Score	Bemerkung /bitte spezifizieren
<b>B. Konkrete Leistung des Insourcers</b>	JA (1) / NEIN (0)	Score	Bemerkung /bitte spezifizieren
<b>C. Kosten</b>	JA (1) / NEIN (0)	Score	Bemerkung /bitte spezifizieren
<b>D. Risiken der Auslagerung</b>			
<b>1. Aufsichtsrechtliche Vorgaben</b>	JA (1) / NEIN (0)	Score	Bemerkung /bitte spezifizieren
<b>2. Eignung des Insourcers</b>	JA (1) / NEIN (0)	Score	Bemerkung /bitte spezifizieren
<b>2. Vertrag</b>	JA (1) / NEIN (0)	Score	Bemerkung /bitte spezifizieren
<b>3. Komplexität</b>	JA (1) / NEIN (0)	Score	Bemerkung /bitte spezifizieren
<b>4. Ausfall des Insourcers (Stunden, Tage, Wochen?) / Abhängigkeit (insbesondere bei Auslagerung von Steuerungs- und Kontrollbereichen)</b>	JA (1) / NEIN (0)	Score	Bemerkung /bitte spezifizieren

  

Kennzahl Reifegrad	Orientierung Auslagerungsvotum	Faktor Reifegrad	Faktor Wesentlichkeit	R-Kennzahl	Risiko-Kategorie
40-50	Empfehlung	0	0	9	wesentlich
21-39	Empfehlung mit Auflagen			8	
0-20	keine Empfehlung			7	nicht wesentlich
				6	
				5	
				4	
				3	
				2	
				1	

  

<b>Aufgaben - ...</b>	Datum	Unterschrift Auslagerungsbeauftragter	Datum	Unterschrift Fachbereichsleiter
-----------------------	-------	---------------------------------------	-------	---------------------------------

## Scoring Detail

**Instituts- / Gruppenweite Risikoanalyse:**  
**Wesentlichkeit & Reifegrad einer Auslagerung** (gemäß MaRisk AT 9 Tz. 2)

Die Bank / das übergeordnete Institut legt in Übereinstimmung mit Ihrer Sourcing-Strategie Instituts-/ gruppenweit die nachfolgend einheitlichen Kriterien fest, nach denen beurteilt wird, ob und inwiefern die ausgelagerten / auszulagernden Dienstleistungen und Prozesse in Bezug auf die Gesamtrisikolage des Instituts "wesentlich" oder "nicht wesentlich" sind". Dabei wird die Wesentlichkeit einer Auslagerung **uniform** anhand der folgenden Analyse ermittelt, die aufsichtsrechtliche und wirtschaftliche Indikatoren kombiniert. Proportionalitätsprinzip - Art und Umfang variieren - das vorliegende Formular ist ein Beispiel und muss demgemäß auf Institut und Vorhaben angepasst werden. Die Systematik der Punktevergabe und Klassifizierung ist ein Beispiel und kann institutsspezifisch ausgelegt werden.

**OUT-SOURCER = Institut, oft bezeichnet als "auslagernes Unternehmen"**     **IN-SOURCER = Dienstleister, oft bezeichnet als "Auslagerungsunternehmen"**

**Dokumentation zur Organisation des Hauses:**

- Auslagerungsstrategie: (Nr.../veröffentlicht...  Ja/  Nein? Eingebunden in die Gesamt-Geschäftsstrategie  Ja/  Nein?)
- Funktion Auslagerungsbeauftragter: (Stellenbeschreibung  Ja/  Nein?)
- Personelle Ausstattung: ((risikoorientierte) Anzahl... FTE (Full-Time Equivalent) inkl. Stellvertretung  Ja/  Nein?)
- Policies, Handbücher und Vorlagen (SFO/Arbeitsanweisung Auslagerung Nr. ...  Ja/  Nein?) (Verankerung mit Fachbereichs-AAW...  Ja/  Nein?)

QUELLE/ KÜMMERER/ AUSFÜLLER		Reifegrad	Wesentlichkeit	
-----------------------------------	--	-----------	----------------	--

Kennzahl Reifegrad	Orientierung Auslagerungsvotum
40-50	Empfehlung
21-39	Empfehlung mit Auflagen
0-20	keine Empfehlung

Faktor Reifegrad	Faktor Wesentlichkeit
31	6

R-Kennzahl	Risiko-Kategorie
9	wesentlich
8	
7	
6	
5	nicht wesentlich
4	
3	
2	
1	

**Auflagen - ...**

Wurden die Ergebnisse gemäß ablauforganisatorischen Regelungen zur Ermittlung der Risiko-Tragfähigkeit des Instituts/der Gruppe veranlasst?  Ja  NEIN

**Reguläres Wiedervorlagedatum:**  
Unwesentliche Auslagerung: aktuelles Datum + max. 1 Jahr;  
Wesentliche Auslagerung < 1 Jahr: 2 bis 4x p.a.:

Hier: \_\_\_\_\_ Hinweis: adhoc Risikoanalysen bei veränderter Risikosituation!!!

Datum	Unterschrift Auslagerungsbeauftragter	Datum	Unterschrift Fachbereichsleiter
-------	---------------------------------------	-------	---------------------------------

## Formular 9.2 Risikoanalyse Auslagerung DETAIL

	C. Kosten	JA (1) / NEIN (0)	Score	Bemerkung /bitte spezifizieren	
<b>Fachabteilung</b> in Zusammenarbeit mit Financin nach Befragung des Dienstleisters	1. Leistung bislang selbst erbracht?	0		Gesetzliche Funktion umgesetzt seit ... Hr. X ist jedoch seit ... krank / im Ruhestand & angemessene Dokumentation ist nicht erfolgt.	
	2. Interne Kosten in €	1		Personalkosten für Beauftragten & Stellvertreter, anteilige Kosten für Arbeiten interner Abteilungen im laufenden Betrieb, Sozialkosten, Raumkosten, IT-Kosten, Fortbildungskosten, Literatur, etc.	
	3. Erwartete externe Kosten & Einsparung in € (Merkposten: Anteilige Kosten für Arbeiten interner Abteilungen im laufenden Betrieb; Projektkosten intern?)	1		Angebot der Firma x (i.H.v. ...) vom ... (Anlage); Interne Personal- und Projektkosten	
	4. Ist die Preiskalkulation verständlich? (Merkposten: Anteilige Kosten für Arbeiten interner Abteilungen enthalten?)	1		Nachvollziehbar, All-in / Fixbetrag oder Orientierung an Messgrößen wie Bilanzsumme? Preissteigerungen vorgesehen?	
<b>D. Risiken der Auslagerung</b>					
<b>Auslagerungsbeauftragter</b> in Zusammenarbeit mit Risiko-Controlling	1. Aufsichtsrechtliche Vorgaben		JA (1) / NEIN (0)	Score	Bemerkung /bitte spezifizieren
	a. Kern- oder Unterstützungsprozesse bezogen auf Bankgeschäfte / Finanzdienstleistungen, § 1 KWG ?	0	0	§1 KWG nicht betroffen	
	b. Wird der Handhabung* von Risiken aus Bankgeschäften bzw. Finanzdienstleistungen aus der Hand gegeben oder wird nur eine Unterstützung eingekauft? (* = Erfassung, Analyse, Begrenzung, Überwachung, Steuerung oder Kontrolle)?	0	0	Die Umsetzungsverantwortung / Handhabung obliegt immer den Fachabteilungen (Erläuterung zu MaRisk AT 4.4.2 Tz. 1)	
	c. Pflichtaufgabe von Seiten der Bankaufsicht? Hilfsfrage: Würde man ohne dies Tätigkeit <u>keine</u> Banklizenz bekommen? Drohen Strafen?	1	1	MaRisk-Compliance ist obligatorisch § 25a, Abs. 1, 3, c KWG i.V.m. MaRisk AT 4.4.2	
<b>Fachabteilung</b> sitzender	2. Eignung des Insourcers		JA (1) / NEIN (0)	Score	Bemerkung /bitte spezifizieren
	a. Firma des Insourcers bekannt?	1		Name des Kaufmanns unter dem die Handelsgeschäfte betrieben	
	b. Anzahl der Mitarbeiter bekannt?	1		50	
	c. Bilanzsummen der letzten 5 Jahre bekannt?	0		Start-Up.	
	d. Bestand (Jahre) der Firma bekannt?	1		Start-Up.	
	e. Bekannt seit wann Dienstleistung angeboten?	1		Start-Up zum ... jedoch Vorbefassung Compliance /Veröffentlichungen -	
	f. Eigentümerstruktur bekannt?	1		Firmen / Verbund / Zentralbank / ? Bilanzsumme ...	
	g. Handelsregisterauszug liegt vor? [Geschäftsleitung / Prokuristen]	1		Start-Up. Bislang keine Wechselfrequenz erkennbar.	
	h. Relevante Zertifizierungen? (ISO 9001, 19600, IDW PS 980, Prüfungsstandard 951/ ISAE 3402, SAS 70 etc.) / Genehmigungen der Aufsicht?	1	1	PS 951	
i. Wesentliche Feststellungen in der Dienstleistungs- erbringung? Kontaktaufnahme mit betroffenem Kunden.	1		Rücksprache erfolgte - Ursache war Nichtinbezug des Insourcers in die Jahresabschlussprüfung durch den Outsourcer => Eigenverschulden.		

Auslagerungsbeauftragter bzw. Fachabteilung in Zusammenarbeit mit Dienstleister

j. Regelung zu (Einzel-/Ketten-) Weiterverlagerung der Dienstleistung enthalten? Steht dies unter einem vorherigen Einverständnisvorbehalt?	1		Es sind Regelungen zur Weiterverlagerung enthalten: Ausgeschlossen ohne vorheriges Einverständnis. Zum Thema Evidenz wurden die gängigen aufsichtlichen Erleichterungen genutzt: Es wurde die Notwendigkeit der Vorlage von uneingeschränkten Bescheinigungen vom Typ B nach IDW PS 951 oder SAS 70 Reports zwischen Insourcer und künftigen Ketten-Insourcern vereinbart und dies/e werden (sofern einschlägig) uns als Outsourcer in gültiger Form vorgelegt. Ebenso wurde die Notwendigkeit der Vorlage relevanter Prüfungsergebnisse und schließlich durch eine Vereinbarung zu Ergänzungsprüfungen für eine künftige Vereinbarung mit dem Ketten-Insourcer abgemacht/getroffen. Diese Vereinbarungen sind ist uns sodann jeweils vorzulegen. [Vgl. "Detail Weiterverlagerung"].
k. Wurden Referenzen / Wirtschaftsseiten / Internetforen geprüft?	1		Telefonate mit 2 Kunden des Insourcers geführt (Management & Sachbearbeiterebene) & branchenbekannt.
l. Durchschnittliche Betriebszugehörigkeit bekannt (Mitarbeiterzufriedenheit / Soziale Compliance)	1		Start-Up. Bislang keine statistischen Daten, Nichts in www.companize.com/arbeitgeberbewertung www.kununu.com, etc. enthalten.
m. Angemessene personelle, technisch-organisatorische Ausstattung vorhanden?	1		Der Insourcer verfügt gemäß übermittelter und beigefügter Aufstellung über ausreichend (hier 5) Beauftragte sowie ausreichende IT-Entwicklerkapazitäten inkl. Stellvertretung.

Auslagerungsbeauftragter in Zusammenarbeit mit Rechtsabteilung, Datenschutzbeauftragtem und IT-Sicherheitsbeauftragtem

2. Vertrag	JA (1) / NEIN (0)	Score	Bemerkung /bitte spezifizieren
a. Auslagerungsverträge - Erfüllen der Vorgaben nach § 25b KWG/MaRisk AT 9 Tz. 6?	1		Die zunächst vorgelegten Verträge wiesen veraltete §§-Angaben auf. Es fehlten KPIs (key performance indicators) und Regelungen für eine unvorhergesehene Beendigung der Auslagerung. Nach Überarbeitung (inkl. exit-support) und vorgelegter Legal Opinion einer unabhängigen Kanzlei werden nun die Vorgaben erfüllt.
b. Vertraglich zugesicherte Fach- / Spezialkompetenz (des Beauftragten)? Insbes. Weiterverlagerungen?	1	1	MaRisk-Compliance: <ul style="list-style-type: none"> <li>• Systematisches Verständnis der für das Institut relevanten rechtlichen Regelungen und Vorgaben mit der Fähigkeit diese anlassbezogen zu vertiefen (z.B. Volljurist, Wirtschaftsjurist, ehem. Revisor, etc. mit 5 Jahren Berufserfahrung im Bankumfeld).</li> <li>• Angemessene Kenntnisse über Organisationsstrukturen und Prozesse des Instituts / Banken generell (z.B. durch vorangegangene Banklehre/Banktätigkeit/Trainee-Programm)</li> </ul> <b>EINBEZUG des Datenschutzbeauftragten ist erfolgt.</b>
c. Vereinbarung über die Definition eines "wesentlichen Mangels" als Ausgangspunkt für eine ad-hoc-Informationspflicht des Insourcers.	1		Vereinbarter Begriff eines wesentlichen Mangels entspricht gängiger Fachliteratur (IDW, GV, Anlage 6 Prüf-BV ...)? "Ein Mangel, der die Wirksamkeit der Präventionsmaßnahme bzw. Präventionsvorkehrung beeinträchtigt".
d. Vertragliche KPIs MaRisk-Compliance inkl. Kündigungsrechte und bei Überschreitung der maximal akzeptablen Schlechtleistung s.u.).	1		<ul style="list-style-type: none"> <li>• Sämtliche Primärpflichten MaRisk-Compliance</li> <li>• Vor-Ort-Termine</li> <li>• Updates über Rechtsänderungen</li> <li>• Erreichbarkeit (tel./mail)</li> <li>• Fachkompetenz</li> <li>• Einhaltung unverzüglicher Information bei wesentlichem Mangel</li> <li>• Jahresbericht</li> <li>• Schulungen</li> <li>• ...</li> </ul>
e. Mangelhafte Leistungserbringung	0		Leistungsumfang ist vertraglich festgelegt (KPIs). Die ausgelagerte Tätigkeit wird von Spezialisten in einem professionellen Umfeld durchgeführt. Eskalationsmechanismus ist enthalten.
f. Datenschutz- IT-Sicherheits geregelt?	0		Mit dem Insourcer sind Regelungen hinsichtlich datenschutzrechtlicher Bestimmungen vertraglich vereinbart worden. <b>Ferner wurde eine Verpflichtung auf die relevanten Vorgaben der MaRisk, z.B. AT 7.2, Technisch- organisatorische Ausstattung, Berechtigungsmanagement, Datentransport, etc. unterzeichnet.</b>
g. Vertragslaufzeit angemessen?	1		<b>Der Vertrag läuft zunächst für 3 Jahre und verlängert sich jährlich zum 31.12. für ein Jahr. Angemessene Kündigungsfristen und Sonderkündigungsregelungen wurden vereinbart.</b>
3. Komplexität	JA (1) / NEIN (0)	Score	Bemerkung /bitte spezifizieren
a. Verlust von Kompetenzen / KNOW-HOW?	1		Denn: Es wurden Schulungen, Abstimmungsgespräche, etc. mit dem Insourcer vertraglich vereinbart. Ebenso ein dezidierter Exit-Support für den Fall eines Re-sourcings. (beabsichtigt & unbeabsichtigt)

Auslagerungsbeauftragter in Zusammenarbeit mit Fachabteilung und Risiko-Controlling	b. Projektdurchführung bei Auslagerung erforderlich??!	1	→	1	Zahlreiche Abteilungen werden zur Umsetzung (Stichwort Risk-Assessment) benötigt werden - => personelle und sachliche Ressourcenbindung i.H.v. x Tagen gesamt.
	c. Komplexität der Auslagerung	1	→	1	Komplexität/Vielschichtigkeit: Hohe Prozessinterdependenz✓ Hoher Grad der Systemunterstützung inkl. Automatisierungsgrad, IT-Schnittstellen. ✓ Vielzahl der ausgelagerten Tätigkeiten✓ Hoher Entscheidungsspielraum Insourcer✓
	d. RISIKO-KONZENTRATION - INTRA-Risikokonzentration? - INTER-Risikokonzentration? - Einfluss auf das Gesamtrisikoprofil oder die Fähigkeit zum Betreiben seines Kerngeschäftes?		→	0	1. Wegen der Auslagerung der MaRisk-Compliance auf EINEN Dienstleister besteht keine INTRA-Risikokonzentration (also ein Gleichlauf von Risiko-Positionen innerhalb einer Risiko-Art), denn auch bei einer internen Darstellung dieser Compliance erfolgt die Bearbeitung zumeist in EINER Einheit des Hauses.  2. Wegen der weiteren Auslagerung der WpHG-Compliance auf DENSELBEN Dienstleister (siehe separate Risikoanalyse vom ...) besteht keine INTER-Risikokonzentration (also ein Gleichlauf von Risiko-Positionen über verschiedene Risiko-Arten hinweg), da hierzu separate Vereinbarungen inkl. Ressourcen, Fachkenntnisse und KPIs getroffen wurden und jeweils separate Zertifizierungen vorgelegt wurden. Weiter erfolgt auch die Steuerung nach 9.7 MaRisk separat. Der Dienstleister hat schließlich KEINE marktbeherrschende Stellung (Kurzform: kein oder nur ungenügender Wettbewerbsdruck / Keine Marktbeherrschungsvermutung da relevanter Marktanteil <40%). 3. Letztlich ist der Einfluss auf das Gesamtrisikoprofil des Hauses oder die Fähigkeit zum Betreiben seines Kerngeschäftes begrenzt, wie die nachstehende Analyse unter 4. zum Ausfall zeigt.
	e. Verlust des Wettbewerbsvorteils?	0			Trifft nicht zu.
	f. Verlust der Kontrolle der Aktivität?	0			Vereinbarung von KPI's / SLAs - siehe separates Formular zu 9.7. MaRisk.
	<b>4. Ausfall des Insourcers (Stunden, Tage, Wochen?) / Abhängigkeit (insbesondere bei Auslagerung von Steuerungs- und Kontrollbereichen)</b>		JA (1) / NEIN (0)		Score
Auslagerungsbeauftragter in Zusammenarbeit mit Fachabteilung und BCM-Beauftragtem	a. Großer Einfluss auf den Geschäftsbetrieb?	0	→	0	MaRisk-Compliance ist vor allem beratend / koordinierende Tätig. Kein Kernprozess des Geschäftsbetriebes.
	c. Auswirkungen auf die BCM-Strategie?	0	→	0	Mangels Auswirkungen wurden keine Notfalltest vereinbart.
	d. Hohe Ergebniswirkung?	0	→	0	MaRisk-Compliance ist kein Profit-Center.
	e. Ersatz nur langfristig möglich?	0	→	0	Eine marktbeherrschende Stellung ist nicht gegeben: Verschiedene Mehrmandanten-Dienstleister bieten die Dienstleistung an. Aufgrund Konkurrenz-Situation ist zügige Bedienung möglich. Übergangsweise kann man sich auch mit kleineren Dienstleistern behelfen, die nur wenige Institute betreuen. [Vgl. hierzu Detail Risikokonzentration sowie Detail Exit-Strategie/Prozedere.] Insgesamt ist nicht von einer Abhängigkeit auszugehen.
		0			

## B. Anforderungen an den Auslagerungsvertrag

Die aufsichtsrechtlichen Anforderungen an die Ausgestaltung eines Auslagerungsvertrages sind mit den aktualisierten Mindestanforderungen an das Risikomanagement<sup>4</sup> (MaRisk 2017) im Vergleich zu der Regelung aus 2012 insgesamt präzisiert worden. Neue Anforderungen betreffen Regelungen zu Kündigungsrechten bei dauerhafter Schlechtleistung sowie zu sonstigen Sicherheitsanforderungen. Die überarbeiteten MaRisk machen deutlich, dass die Risikocontrolling-, Compliance- und Revisionsmechanismen vollumfänglich auch für Subauslagerungen gelten.

Nach einer Befragung der Unternehmensberatung Procedera Consult GmbH zur MaRisk-Novelle 2017 schätzen 67 % der Banken den Änderungsbedarf an Auslagerungsverträgen als sehr stark oder stark ein.<sup>5</sup>

Das vorliegende Dokument beschreibt die Anforderungen an die Vertragsgestaltung und schlägt konkrete Formulierungen für einen Auslagerungsvertrag vor. Um die Formulierungsvorschläge praktisch nutzbar zu machen, gliedert sich das Dokument in die mögliche Struktur eines Vertrages. Der Bundesverband der Deutschen Volksbanken und Raiffeisenbanken (BVR) hat Mustervertragsklauseln<sup>6</sup> zur Thematik Steuerung und Kontrolle des ausgelagerten Bereiches entwickelt. Die Formulierungsvorschläge der Abschnitte B.I.2.a) bis d) orientieren sich an diesen Mustervertragsklauseln.

Für alle Vertragsbestandteile, die nicht durch BVR-Mustervertragsklauseln abgedeckt sind, erfolgen eigene Formulierungsvorschläge.

Nicht betrachtet werden die Teile eines typischen Vertragswerkes, die von der MaRisk unberührt sind. Dabei handelt es sich um die Themen Vergütung der Leistungen (Preise, Rechnungslegung, Fälligkeit), Laufzeit, Schriftform, Geheimhaltung und salvatorische Klausel. Nicht diskutiert werden weiterhin spezielle Anforderungen für Banken, die besonders groß oder deren Geschäftsaktivitäten nach AT (Allgemeiner Teil) 1 TZ (Textziffer) 3 MaRisk durch besondere Komplexität, Internationalität oder Risikoexponierung gekennzeichnet sind.

Die nachfolgenden Ausführungen beschreiben den Fall einer Auslagerung, die im Rahmen einer Risikoanalyse als wesentlich eingestuft wurde. Aber auch unwesentliche Auslagerungen oder Leistungen, die tatbestandlich keine Auslagerungen sind (z. B. sonstiger Fremdbezug von Leistungen), sind im Rahmen von § 25a Abs. 1 KWG in die Gesamtrisikosteuerung des Institutes einzubeziehen. Entsprechend dem Grundsatz der Proportionalität können bei kleinerem Umfang, niedrigerer Komplexität oder Risikogehalt der ausgelagerten Aufgaben die Anforderungen an das Risikomanagement reduziert werden. Die Regelungen im Auslagerungsvertrag sind entsprechend anzupassen.

<sup>4</sup> BaFin: Rundschreiben 09/2017 – Mindestanforderungen an das Risikomanagement, [https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2017/rs\\_1709\\_marisk\\_ba.html?nn=9450904](https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2017/rs_1709_marisk_ba.html?nn=9450904)

<sup>5</sup> Procedera Consult GmbH: Studie zur MaRisk-Novelle 2017, <https://www.it-finanzmagazin.de/studie-zur-marisk-novelle-2017-68-prozent-der-banken-wollen-mehr-auf-it-outsourcing-setzen-47324/>

<sup>6</sup> BVR: Rechtliche Anforderungen an das Outsourcing, Stand 17.10.2017, <https://intern.bvr.de/e.nsf/index.xsp?documentId=F99A5D00133D12D8C1257CF9002EC270>

Im Dokument wird sprachlich unterschieden zwischen dem Institut, dem auslagernden Unternehmen (ff. Auftraggeberin genannt) und dem Auslagerungsunternehmen, das als Dienstleister die ausgelagerten Aufgaben ausführt (ff. Auftragnehmerin genannt). Auftraggeberin und Auftragnehmerin zusammen werden als Vertragsparteien bezeichnet.

In Abschnitt B.I.6 erfolgt ein praxisbewährter Vorschlag, wie beide Vertragsparteien ihren Aufwand zur Steuerung und Kontrolle der Auslagerung deutlich reduzieren können: Eine **„erweiterte“ Zertifizierung der ausgelagerten Aufgaben nach IDW PS 951 Typ B**.

## I. Pflichtangaben

Hinsichtlich der Strukturierung eines Auslagerungsvertrages gibt es keine expliziten Anforderungen in der MaRisk. Gleichwohl hat sich in der Praxis ein Rahmengeschäftsbesorgungsvertrag mit folgenden Anlagen bewährt:

- Konventionen für Leistungsscheine
- Leistungsscheine (Leistungsbeschreibungen)
- Kommunikationsmatrix
- Auftragsdatenverarbeitung i. S. d. § 11 Abs. 2 Bundesdatenschutzgesetz
- Reporting
- Request for Change-Formblatt

Die Kommunikationsmatrix ist eine Übersicht über Ansprechpartner, Rollen, Verantwortlichkeiten und Kommunikationswege beider Vertragsparteien. Die Definition klarer Verantwortlichkeiten ist nach AT 4.3.1 TZ 2 der MaRisk (Aufbau- und Ablauforganisation) verpflichtend.

## 1. Vertragsgegenstand und Leistungspflichten der Auftragnehmerin

### a) Grundlagen

Bei umfangreicheren Dienstleistungen empfiehlt es sich, den Vertragsgegenstand nicht detailliert im Auslagerungsvertrag, sondern als Anlagen in Leistungsscheinen zu beschreiben. Im Vertrag reicht dann eine grobe, stichwortartige Aufzählung der Dienstleistungen.

Nach § 25b KWG Abs. 2 darf die Auslagerung nicht zu einer Übertragung der Verantwortung der Geschäftsleiter an die Auftragnehmerin führen. Der Auslagerungsvertrag sollte daher einen Passus enthalten, der das grundlegende Verhältnis von Auftraggeberin und Auftragnehmerin beschreibt.

#### Formulierungsvorschlag:

Gegenstand dieses Vertrages ist <grobe Aufzählung der Dienstleistungen>. Eine Delegation der Verantwortung der Geschäftsleitung der Auftraggeberin an die Auftragnehmerin oder die Übertragung von Leitungsaufgaben der Geschäftsleitung sind nicht Gegenstand dieses Vertrags und können nicht wirksam vereinbart werden. Gleiches gilt für erlaubnispflichtige Bank- und Finanzdienstleistungen im Sinne des § 32 KWG.

Im Übrigen erfolgt die Erbringung der Dienstleistungen aus Sicht der Auftraggeberin nach den Outsourcing-Bedingungen der Mindestanforderungen an das Risikomanagement (MaRisk).