Riediger (Hrsg.)

Auslagerungen und Dienstleister-Steuerung

Aktuelle Anforderungen aus DORA, KWG, EBA-Guidelines und MaRisk/BAIT im Umgang mit Auslagerungen für signifikante und weniger signifikante Institute

3. Auflage

FCH AG, 2025

Riediger (Hrsg.)

Auslagerungen und Dienstleister-Steuerung

Aktuelle Anforderungen aus DORA, KWG, EBA-Guidelines und MaRisk/BAIT im Umgang mit Auslagerungen für signifikante und weniger signifikante Institute

3. Auflage

Khalid Ahmad
DOR-Beauftragter
Abteilungsleiter Business Resilience
Deutsche WertpapierService Bank AG

Sven Chudzinski
Bereichsleiter Controlling, Meldewesen und
Zentrales Auslagerungsmanagement
Volksbank im Bergischen Land eG

Larissa Eigenwillig
Consultant Kompetenzteam Compliance
AWADO GmbH Wirtschaftsprüfungsgesellschaft
Steuerberatungsgesellschaft

Michael Gastmann
Auslagerungsbeauftragter/Datenschutzbeauftragter
Stabsstelle Überwachungsmanagement
Volksbank im Münsterland eG

Roland Hein
Geschäftsführer
bit Informatik GmbH

Maximilian Herting
Wissenschaftlicher Mitarbeiter
AWADO Rechtsanwaltsgesellschaft mbH &
Universität Osnabrück

Johannes Hugo
Leiter Competence Center Information Security
x1F GmbH

Barbara Hugo-Dilworth
Head of Outsourcing Management
IKB Deutsche Industriebank AG

Michael Kirschbaum
Referent Zentrales Auslagerungsmanagement
LBBW

Daniel Krüger
Rechtsanwalt
AWADO Rechtsanwaltsgesellschaft mbH

Christoph Leibnitz
Zentraler Auslagerungsbeauftragter
Sparkasse Mülheim an der Ruhr

Oliver Michelmann
Fachprüfer im Referat Bankgeschäftliche Prüfungen
Deutsche Bundesbank, Hannover

Markus Müller
Independent Compliance Risk Management
Germany MaRisk-Compliance Monitoring/
Deputy Head MaRisk-Compliance
Citigroup Global Markets Deutschland AG

Stefan Nikula
Abteilungsleiter Gesamtbanksteuerung
Salzlandsparkasse

Henning Riediger (Hrsg.)
Prüfungsleiter, Referat Bankgeschäftliche Prüfungen
Deutsche Bundesbank, Hannover

Pascal Ritz LL.M.
Geschäftsführer
Justo Unternehmensberatung GmbH
Compliance-Spezialist

Ingvar Rosenhagen
Bereichsleiter IT-Governance
ALTE LEIPZIGER Lebensversicherung auf Gegenseitigkeit

Selina Schubert, LL.M.
Consultant Kompetenzteam Compliance
AWADO GmbH Wirtschaftsprüfungsgesellschaft
Steuerberatungsgesellschaft

Kathrin Stein
Leiterin Interne Revision
Sparda-Bank München eG

Peter Uherr
Director, Leiter Compliance
AWADO GmbH Wirtschaftsprüfungsgesellschaft
Steuerberatungsgesellschaft

Kay Wachelau
Auslagerungsbeauftragter | Beauftragter für IKT-Drittparteien
DONNER & REUSCHEL Aktiengesellschaft

FCH AG, 2025

Inhaltsübersicht

Inhaltsverzeichnis

A.

Einleitung

A. Einleitung[1]

I. Vorüberlegungen

Was haben Auslagerungen und die Raumfahrt gemeinsam? Auf den ersten Blick nicht allzu viel. Jedoch eine elementare Eigenschaft zeichnet beide aus: das Andocken. Wie beim Andocken an der Internationalen Raumstation ISS ist es bei der Auslagerung wichtig, dass die ausgelagerten Aktivitäten und Prozesse weiterhin mit dem Institut respektive dem Internen Kontrollsystem verbunden sind. 1

Diesem Andock-Prozess wird auch mit der 3. Auflage wieder angemessen Rechnung getragen, um sich umfassend mit den Anforderungen und deren Umsetzung in der Praxis zu befassen. Wie schon in den Vorauflagen wird sodann deutlich, dass die Auslagerung allein keinen Selbstzweck verfolgt, sondern mittlerweile insbesondere im IT-Bereich für das Betreiben des Bankgeschäfts von elementarer Bedeutung ist. Diesem symbiotischen Zusammenhang folgend ist die Einbeziehung von Auslagerungen in das Interne Kontrollsystem geboten. Nicht nur die internen (Geschäfts-)Prozesse bedürfen einer regelmäßigen und angemessenen Überwachung, sondern auch die ausgelagerten Komponenten. Diese Sichtweise wird auch seit Jahren von qualitativen Anforderungen der Regulierungsbehörden, insbesondere der Bankenaufsicht, gefordert und findet sich in den einschlägigen Regelungen. Hierzu zählen neben der EU-Verordnung DORA[2] (Digital Operational Resilience Act) für den gesamten Finanzsektor auch die entsprechenden EBA-Leitlinien zur Auslagerung[3], sowie die jeweiligen sektorspezifischen nationalen Regelungen, im Bankensenktor z. B. in den MaRisk[4] sowie in Teilen spezifischer in den BAIT[5]. 2

Idealerweise fängt die Auslagerungsthematik bereits in der Strategie mit der Definition von klaren überprüfbaren Aussagen an und leitet über den Informationsrisikomanagementprozess zum Auslagerungsmanagementprozess über. 3

1 Die nachfolgenden Interpretationen und Meinungen sind ausschließlich persönliche Auffassungen des Autors und stellen keine offizielle Meinungsäußerung der Deutschen Bundesbank dar.

2 Vgl. *EU* (2022): Verordnung (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor (Digital Operational Resilience Act) vom 14.12.2022, Anwendung ab dem 17.01.2025.

3 Vgl. *EBA* (2019).

4 Vgl. *BaFin* (2024a).

5 Vgl. *BaFin* (2021b).

4 In der Praxis ist vor allem die Diskussion über die Hierarchie von Schutzzielen von Relevanz. Es ist unstrittig, dass die Informationstechnologie möglichst jederzeit zur Verfügung stehen sollte. Um dieses Schutzziel zu erreichen, haben mithin viele Institute oder deren Auslagerungsmandanten erhebliche Ressourcen in die IT-Infrastruktur investiert. Derjenige, der an dieser Stelle die Diskussion mit dem Verweis abbricht, alles getan zu haben, droht zu ignorieren, dass sich die angemessene Steuerung und Überwachung operationeller Risiken im IT-Bereich nicht allein mit dem Schutzziel Verfügbarkeit erreichen lässt. Mindestens ebenso wichtig sind die weiteren Schutzziele Integrität, Authentizität und Vertraulichkeit der Daten. Was nützt es einem Institut, auf verfügbaren Systemen von Dienstleistern zu arbeiten, wenn gleichzeitig nicht sichergestellt werden kann, dass die Veränderbarkeit von Daten in einem fest vordefinierten Umfeld erfolgt? Um dies zu vermeiden, müssen Schreib- (Integrität, Authentizität) und Leserechte (Vertraulichkeit) an Daten einem kontrollierten Benutzerberechtigungsvergabeprozess anhand eines Sollkonzeptes folgen. Die anschließende Kontrolle in Form der Rezertifizierung der eingeräumten Benutzerberechtigungen ist eine Kernkomponente des Internen Kontrollsystems im IT-Bereich sowohl im Institut als auch bei ausgelagerten Aktivitäten.

5 Gleichwohl wie gut die einzelnen Schutzziele verfolgt und erreicht werden, kann eine 100%ige Sicherheit – auch unter betriebswirtschaftlichen Aspekten – weder vom Institut noch vom Dienstleister erwartet werden, so dass die Geschäftsleitung eines Instituts permanent mit der Steuerung der verbleibenden operationellen (Rest-)Risiken – auch beim Dienstleister – konfrontiert ist.

II. Aufbau des Werkes

6 In den folgenden Buchabschnitten möchten die Autoren Ihnen Anregungen für verschiedene Ausprägungen des Internen Kontrollsystem für den Auslagerungsbereich aufzeigen, welche nach aufsichtlichem Verständnis ebenfalls geboten sind.

7 Die Anforderungen sind dem Grunde nach selbstverständlich auf jedes Auslagerungsverhältnis übertragbar, jedoch jeweils immer vor dem Hintergrund der Angemessenheit zu beurteilen. Wichtig ist in diesem Zusammenhang zudem der gesunde Menschenverstand. Hierzu ein vereinfachtes Beispiel: Während von einem IT-Mehrmandantendienstleister eine vierteljährliche Risikoberichterstattung verlangt werden kann, ist eine analoge Forderungsübertragung auf Werttransportunternehmen utopisch. In diesen Fällen müssen andere geeignete

Instrumente angewandt werden, um sicherzustellen, dass Veränderungen in der Risikostruktur spätestens nach einem Quartal deutlich werden.

Das vorliegende Buch beginnt zunächst mit einer Beschäftigung mit dem Thema Auslagerung aus der bankaufsichtlichen Perspektive im **Kapitel B** und stellt zentrale Aspekte eines angemessenen Risikomanagements im Umgang mit Auslagerungen dar. Eine Vielzahl von praxisrelevanten Hinweisen bietet dem Leser die Möglichkeit, Fallstricke und wiederkehrende Schwäche zu erkennen und nachhaltig auszuschließen. Zudem wird auf die Chancen und Risiken durch die DORA-Verordnung eingegangen. 8

Anschließend widmet sich das **Kapitel C** dem Thema der Risikoanalyse von Auslagerungen. Verbunden ist diese Thematik immer mit der Frage nach Wesentlichkeit der Auslagerung. In diesem Abschnitt erhalten Sie wertvolle Hinweise zur praktischen Umsetzung und Implementierung von Schnittstellen zwischen den einzelnen Prozessschritten und/oder beteiligten Organisationseinheiten. Gegenüber der Vorauflage wurde der Abschnitt um die spezifischen Anforderungen an Signifikante Institute (sog. SIs) erweitert, um zum einen den erhöhten Anforderungen an diese Klasse von Instituten Rechnung zu tragen und zum anderen die Anwendung des Proportionalitätsgedankens noch stärker als bisher aufzuzeigen. 9

In **Kapitel D** erfolgt die umfassende Auseinandersetzung mit dem Themenschwerpunkt DORA. In diesem Kapitel werden die nunmehr finanzmarktweit geltenden Regelungen an die Informationstechnologie aufbereitet und mögliche Handlungsoptionen dargelegt. Insbesondere für IT-Auslagerungen erfordern die neuen Anforderungen ein deutlich breiteres Befassungsspektrum als dies bisher in der Bankpraxis flächendeckend vorzufinden war. 10

Anschließend erfolgt in **Kapitel E** die Betrachtung des Aufbaus einer angemessenen Dienstleister-Steuerung. Hierzu wird zunächst der rechtliche Rahmen umfassend abgesteckt und auf das erforderliche Zusammenspiel der Funktionen in den Instituten abgestellt. Im Anschluss wird anhand von Praxisbeiträgen der Aufbau einer Auslagerungssteuerung einer Bank und einer Versicherung vorgestellt und vertieft. 11

Das **Kapitel F** beschäftigt sich vorrangig mit dem Thema der Auslagerbarkeit von zentralen Komponenten des Risikomanagements. Gerade besondere Funktionen, wie die Risikocontrolling- und Compliance-Funktion sowie die Interne Revision, sind nicht uneingeschränkt auslagerbar. Jedoch gerade vor dem Hintergrund der bankaufsichtlich propagierten »Doppelten Proportionalität« 12

ergeben sich nutzbare Spielräume. Interessant wird es insbesondere bei der Begrenzung dieser Spielräume.

13 Eine Besonderheit im Bereich der Auslagerungen stellt die Übertragung der Funktion des IT-Sicherheitsbeauftragten dar und wird daher im **Kapitel G** entsprechend gewürdigt. Dabei wird insbesondere die Sensibilität dieser Auslagerungsoption aufgezeigt.

14 Das **Kapitel H** setzt sich mit dem Thema der Integration von ausgelagerten Aktivitäten in dem Internen Kontrollsystem auseinander. Es erfolgt eine umfassende Aufbereitung der Schnittstellen im Internen Kontrollsystem über die alleinigen Auslagerungsanforderungen des AT 9 der MaRisk hinaus.

15 Welche Aktivitäten zur Überwachung der Einhaltung vertraglicher, regulatorischer und gesetzlicher Anforderungen vorgenommen werden sollte, ist Bestandteil des **Kapitels I**, welches sich praxisorientiert mit den entsprechenden Kontrollhandlungen auseinandersetzt und entsprechende Handlungsoptionen vorbereitet.

16 Grundsätzlich besteht die Erwartung, dass beim Dienstleister »alles rund läuft«. Da dies – wie im eigenen Haus – nicht immer 100%ig klappt, setzt sich das folgende **Kapitel J** mit dem Thema Handlungsoptionen und Notfallpläne intensiv auseinander und stellt verschiedene Alternativen zum Umgang vor.

17 Ein zentrales Thema im Umgang mit Auslagerungen besteht in der Weiterverlagerung. Gerade solche Auslagerungsketten begünstigen das Eintreten einer »Aus den Augen, aus dem Sinn«-Mentalität. Hier gilt es jedoch vorzubeugen und sich den Herausforderungen zu stellen. Im **Kapitel K** erhalten Sie dazu umfangreiche Informationen zum erfolgreichen Umgang mit Weiterverlagerungen.

18 Die Aspekte der Steuerung und Überwachung von Dienstleistern stehen im Vordergrund des **Kapitels L**, welches sich mit der Überwachung der Einhaltung vertraglicher, regulatorischer und gesetzlicher Anforderungen beim Dienstleister auseinandersetzt. Auch an dieser Stelle wird dem Proportionalitätsgedanken Rechnung getragen, sodass jeweils ein Beitrag mit dem Schwerpunkt SI und ein Beitrag mit dem Schwerpunkt LSI[6] Eingang in das Werk gefunden haben.

6 LSI = less significant institution, weniger bedeutendes Institut im Sinne des SSM-Verständnisses der europäischen Bankenaufsicht.

Neben den bisherigen Themen des Internen Kontrollsystems kommt der Revisionstätigkeit als zweites Standbein der Internen Kontrollverfahren eine herausgehobene Position zu. An welchen Stellen die Revision tätig werden soll, ist Bestandteil des **Kapitels M**. Das Vorgehen und Zusammenwirken im Risikomanagement werden umfassend erläutert und eine Vielzahl an praktischen Hilfestellungen gegeben. 19

Zum Abschluss dieses Werkes wird im **Kapitel N** noch auf den aufsichtlichen Umgang mit Auslagerungen im Bereich der Kapitalfestsetzung und im Rahmen von Bankgeschäftlichen Prüfungen eingegangen. 20

Insgesamt handelt es sich – auch in der 3. Auflage – um ein Praktikerhandbuch, welches die Lösung der Aufgaben voranstellt. Teilweise ist es jedoch erforderlich, zunächst eine gewisse Problemsensibilität zu entfalten. Aber wenn Sie es schon bis hierher geschafft haben, dann sollte Problemsensibilität nicht unbedingt eine fehlende Eigenschaft sein. 21

Ich wünsche Ihnen viel Spaß beim Lesen und die erfolgreiche Verprobung mit Ihren eigenen institutsinternen Vorgehensweisen und Verfahren. 22

Glück Auf!

B.

Begriffsbestimmung und Abgrenzungstatbestand

B. Begriffsbestimmung und Abgrenzungstatbestand[7]

I. Bedeutung der Auslagerung im Internen Kontrollsystem

1. Vorbemerkungen

Das folgende Kapitel fokussiert sich zunächst auf die allgemeinen Anforderungen an Auslagerungsverhältnisse aus Sicht der MaRisk und somit aus Sicht einer Bank, kann aber im Wesentlichen auf andere Teilnehmer des Finanzmarktes übertragen werden. Spezifische Anforderungen im Informationstechnologie-Bereich werden entsprechend ausgeführt. Mit Anwendung von DORA ab dem 25.01.2025 gelten im IT-Auslagerungsbereich zusätzliche Anforderungen. Zu deren detaillierten Handhabung wird auf das Kapitel D verwiesen. Gleichwohl plant die Aufsicht gemäß dem Anschreiben zur letzten MaRisk-Novelle vom 29.05.2024[8], die die aktuell gültigen bankaufsichtlichen bzw. zahlungsdiensteaufsichtlichen/versicherungsaufsichtlichen/kapitalverwaltungsaufsichtlichen Anforderungen an die IT (BAIT, ZAIT, VAIT und KAIT) aufzuheben, um eine Doppelregulierung zu vermeiden. Zudem ist zu beachten, dass der Text der DORA-Verordnung noch um weitere Spezifikationen der EBA (sog. ITS – Implementierungsstandards sowie RTS – Regulatory Technical Standards) erweitert werden wird. 23

Aufgrund des finanzsektorübergreifenden Charakters der DORA sind alle drei europäischen Aufsichtsbehörden (EBA, EIOPA, ESMA)[9] gemeinsam beauftragt worden, Entwürfe für die technischen Regulierungs- und Durchführungsstandards der EU-Kommission vorzulegen. RTS und ITS, die bisher als finale Berichte der Entwürfe durch die ESAs vorliegen, werden im weiteren Prozess von der Europäischen Kommission noch angenommen und geprüft, bevor sie im Amtsblatt der EU veröffentlicht werden. 24

7 Autor: *Henning Riediger*. Die nachfolgenden Interpretationen und Meinungen sind ausschließlich persönliche Auffassungen des Autors und stellen keine offizielle Meinungsäußerung der Deutschen Bundesbank dar.

8 Vgl. *BaFin* (2024a), Anschreiben sowie die erfolgte Umsetzung im Januar 2025, vgl. BaFin (2025), mit der Aufhebung von BAIT, KAIT und ZAIT mit Ablauf des 16.01.2025 und für die BAIT mit der Änderung des Anwenderkreises: Banken bzw. Kreditinstitute, die DORA umsetzen müssen, gelten die MaRisk mit Ablauf des 16.01.2025 nicht mehr, anderenfalls gilt die Aufhebung der BAIT zum 31.12.2026.

9 EBA = Europäische Bankenaufsichtsbehörde, EIOPA = Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung, ESMA = Europäische Wertpapier- und Marktaufsichtsbehörde.

25 Die MaRisk fordern den Aufbau Interner Kontrollverfahren, welche sich wiederum aus dem Internen Kontrollsystem und der Internen Revision zusammensetzen (vgl. Abbildung B-1). Die Aufgabe des Internen Kontrollsystems ist de facto die Kontrolle der eingerichteten Prozesse und Überwachungsaufgaben. Die Kontrollen dienen mithin dem Ziel, Fehler, Schwachstellen und Mängel im Prozess transparent zu machen und dem Management die Möglichkeit zu bieten, korrigierend einzugreifen. Hingegen sollten die Aufgaben der Internen Revision sich darauf konzentrieren, zu beurteilen, ob das eingerichtete Interne Kontrollsystem funktionsfähig ist. Losgelöst von der idealtypischen Aufgabenverteilung ist in der Praxis häufig festzustellen, dass die eigentlich im Internen Kontrollsystem zu erwartenden Kontrollhandlungen durch die Interne Revision wahrgenommen werden. Derartige Funktionstrennungsverstöße führen im Ergebnis zu einer Einschränkung der Unabhängigkeit der Internen Revision, da die entsprechenden Prüfungshandlungen in der Folge entweder nicht mehr durchgeführt werden oder es aber zu einer nicht zweckmäßigen Überprüfung der eigenen Tätigkeiten kommt.

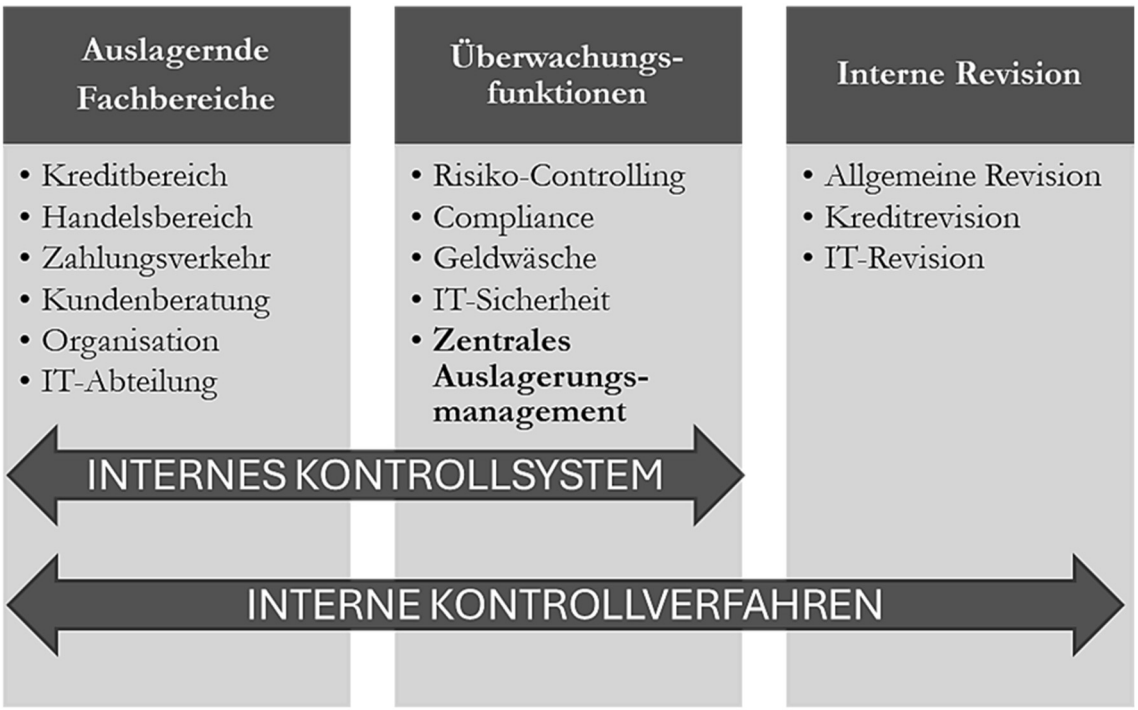

Abbildung B-1: Konzept der drei Verteidigungslinien bei Auslagerungen.[10]

26 Die Fachbereiche, welche das »Tagesgeschäft« mit den integrierten Kontrollen (z. B. Vier-Augen-Prinzip) abwickeln, stellen nach diesem Konzept die erste

10 Quelle: Eigene Darstellung.