Riediger (Hrsg.)

Auslagerungen und Dienstleister-Steuerung

2. Auflage

Finanz Colloquium Heidelberg, 2020

Zitiervorschlag:

Autor in: Riediger (Hrsg.): Auslagerungen und Dienstleister-Steuerung 2. Auflage, RdNr. XX.

ISBN: 978-3-95725-166-4

Finanz Colloquium Heidelberg GmbH
Im Bosseldorn 30, 69126 Heidelberg
www.FCH-Gruppe.de
info@FCH-Gruppe.de
Titelfoto: Silberberg GmbH Montafon
Satz: MetaLexis, Niedernhausen
Druck: Grafisches Centrum Cuno GmbH & Co. KG, Calbe

Riediger (Hrsg.)

Auslagerungen und Dienstleister-Steuerung

2. Auflage

Dirk Busenbach
Abteilungsleiter
Organisation/Verhinderungsvertreter des Vorstands
Sparkasse Gummersbach-Bergneustadt
Gummersbach

Roland Hein
Geschäftsführer bit Informatik GmbH
Trier

Volker Köster
Direktor Organisation &
Informationssicherheits-Beauftragter
Kreissparkasse Verden
Verden

Christoph Leibnitz
Verantwortliche Stelle für
Auslagerungsmaßnahmen, Dienstleister-Steuerung
Sparkasse Mülheim an der Ruhr
Mülheim

Robert Plaßmann
Prokurist Deutsche Apotheker- und
Ärztebank
Düsseldorf

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

Pascal Ritz LL.M.
Compliance-Spezialist,
u. a. für die FCH Compliance tätig

Lukas Walla
Regulatorik/Compliance
Investitionsbank Schleswig-Holstein

Finanz Colloquium Heidelberg, 2020

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

Es 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. 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 (vgl. BAIT Tz. 1 f.). 3

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- (In- 4

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

tegrität, Authentizität) und Leserechte (Vertraulichkeit) an Daten einem kontrollierten Benutzerberechtigungsvergabeprozess anhand eines Sollkonzeptes folgen (vgl. BAIT Tz. 24). 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 (vgl. BAIT Tz. 27).

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.

8 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.

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. 9

Das **Kapitel D** 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« ergeben sich nutzbare Spielräume. Interessant wird es insbesondere bei der Begrenzung dieser Spielräume. 10

Das Thema bzw. die Anforderung einer Dienstleister-Steuerung ist ja grundsätzlich nicht neu. Nur seit der letzten MaRisk-Novelle wird dies von den Instituten auch explizit gefordert, so dass das **Kapitel E** hier wertvolle Praxistipps für die Implementierung und Umsetzung bereithält. 11

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 F** mit dem Thema Handlungsoptionen und Notfallpläne intensiv auseinander und stellt verschiedene Alternativen zum Umgang vor. 12

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 G** erhalten Sie dazu umfangreiche Informationen zum erfolgreichen Umgang mit Weiterverlagerungen. 13

Die Aspekte der Steuerung und Überwachung von Dienstleistern stehen im Vordergrund des **Kapitels H**, welches sich mit der Überwachung der Einhaltung vertraglicher, regulatorischer und gesetzlicher Anforderungen beim Dienstleister auseinandersetzt. 14

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 I**. Das Vorgehen und Zusammenwirken im 15

Risikomanagement werden umfassend erläutert und eine Vielzahl an praktischen Hilfestellungen gegeben.

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

17 Insgesamt handelt es sich – auch in der 2. 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.

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

Glück Auf!

B.

Begriffsbestimmung und Abgrenzungstatbestand

B. Begriffsbestimmung und Abgrenzungstatbestand[2]

I. Bedeutung der Auslagerung im Internen Kontrollsystem

1. Vorbemerkungen

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. 19

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

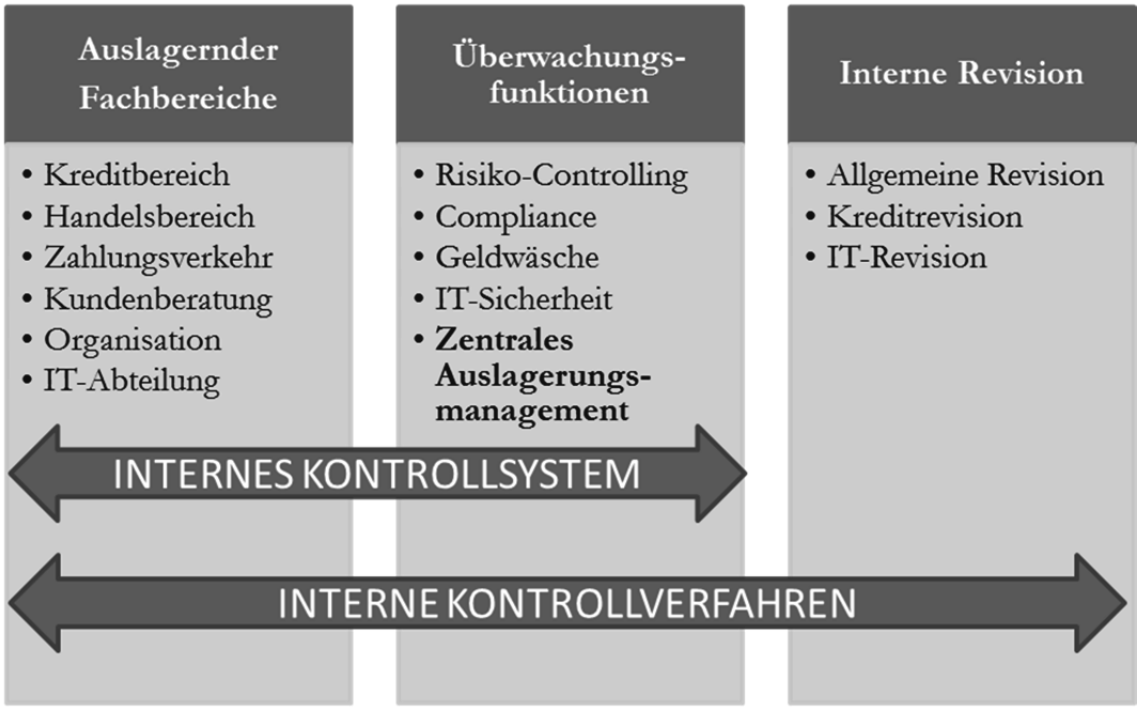

Abbildung B.1: Konzept der drei Verteidigungslinien bei Auslagerungen[3]

20 Die Fachbereiche, welche das »Tagesgeschäft« mit den integrierten Kontrollen (z. B. Vier-Augen-Prinzip) abwickeln, stellen nach diesem Konzept die erste Verteidigungslinie dar. Die zweite Verteidigungslinie in Form der Überwachungs- bzw. Beauftragtenfunktionen soll sicherstellen, dass die eingerichteten Kontrollen wirksam und angemessen ausgestaltet sind. Über diese reine Kontrollfunktion hinaus sind die Funktionen auch an der Weiterentwicklung des Internen Kontrollsystem maßgeblich beteiligt bzw. notwendigerweise hinzuzuziehen. Die Einbindung kann sich über die Methodenentwicklung, die Durchführung von Prozessrisikoanalysen und letztendlich Beratung der Fachbereiche erstrecken. Ihnen kommt somit nicht nur eine reine Kontrollfunktion, sondern ebenso die Funktion eines Ideen- und Impulsgebers bzw. Optimierers zu. Für den IT-Bereich des Internen Kontrollsystems sind hierbei vor allem der IT-Sicherheitsbeauftragter sowie auch der Compliance-Beauftragte gefordert. In einem weiteren Schritt, wenn es insgesamt um die gesamtweite Beurteilung der bestehenden bzw. eingegangenen Risikopotenziale geht, kommt das Risikocontrolling hinzu.

21 Im Entwurf für die 5. MaRisk-Novelle war bereits ein Auslagerungsbeauftragter vorgesehen. In der endgültigen Novelle fällt diese Aufgabe dem **zentralen Auslagerungsmanagement** gemäß AT 9 Tz. 12 der MaRisk zu. Dieser wird erwartungsgemäß den Überwachungsfunktionen zugewiesen werden. Die

3 Eigene Darstellung.