

Riediger (Hrsg.)

Auslagerungen und Dienstleister-Steuerung

2. Auflage

Zitiervorschlag:

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

ISBN: 978-3-95725-166-4
© 2020 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

Inhaltsübersicht

A. Einleitung (<i>Riediger</i>)	1
B. Begriffsbestimmung und Abgrenzungstatbestand (<i>Riediger</i>)	7
C. Risikoanalysen zur Wesentlichkeitseinstufung von Auslagerungen (<i>Köster</i>)	59
D. Auslagerbarkeit von Kontroll- und Kernbankbereichen (<i>Platzmann/Riediger</i>)	93
E. Aufbau einer Dienstleister-Steuerung (<i>Hein</i>)	109
F. Handlungsoptionen und Notfallpläne bei Beendigung der Auslagerung (<i>Busenbach</i>)	147
G. Berücksichtigung von Weiterverlagerungen im Auslagerungsvertrag (<i>Leibnitz</i>)	171
H. MaRisk-Compliance: Überwachung der Einhaltung vertraglicher, regulatorischer und gesetzlicher Anforderungen an Auslagerungen (<i>Ritz</i>)	189
I. Plausibilitäts- und Prüfungspflichten der Internen Revision vor, während und nach der Auslagerung (<i>Walla</i>)	215
J. Bankaufsichtliche Überwachung von Auslagerungsprozessen (<i>Riediger</i>)	241
K. Literaturverzeichnis	251
L. Stichwortverzeichnis	255

Inhaltsverzeichnis

A. Einleitung	1
I. Vorüberlegungen	3
II. Aufbau des Werkes	4
B. Begriffsbestimmung und Abgrenzungstatbestand	7
I. Bedeutung der Auslagerung im Internen Kontrollsystem	9
1. Vorbemerkungen	9
2. Abgrenzung Auslagerung und Fremdbezug	12
3. Strategische Vorgaben zum Umgang mit Risiken aus Auslagerungen und Standards	15
4. Risikoinventur und Risikoanalysen	17
II. Schwerpunkt bei Auslagerungsthemen sind die Informationstechnologie und deren Schnittstellen	21
1. Allgemeine Aspekte	21
2. Einbindung von IT-Auslagerungen in das Informationsrisikomanagement	25
3. Schnittstelle zum Benutzerberechtigungsmanagement	32
4. Schnittstellen zum Notfallmanagement	36
III. Überwachung des Dienstleisters	39
1. Auslagerungsüberwachung im Internen Kontrollsystem	42
2. Überprüfung der Auslagerung durch die Interne Revision	48
IV. Auswirkungen der neuen EBA-Guideline	53
1. Auslagerungsbegriff	53
2. Auslagerungsregister	54
3. Auslagerungsbegriff Zugangs-, Informations- und Prüfungsrechte	56
4. Vereinfachungen für Gruppen und institutsbezogene Sicherungssysteme	57
5. Interessenskonflikte	57

C. Risikoanalysen zur Wesentlichkeitseinstufung von Auslagerungen	59
I. Einstufung in wesentliche und nicht wesentliche Auslagerungen	61
1. Einleitung	61
2. Abstimmung der Inhalte der Risikoanalyse im Institut	62
3. Aufgaben im Zusammenhang einer Risikoanalyse bei der Auslagerung von Aktivitäten und Prozessen	63
4. Risikoerhebung und -bewertung	64
5. Feststellen der Wesentlichkeit einer Auslagerung	68
6. Auslagerungen von erheblicher Tragweite gemäß AT 9.2 der MaRisk	69
7. Auslagerung von IT-Dienstleistungen	70
8. Beispiel – Risikoanalyse auf Basis der Risikokategorisierung der MaRisk (AT 2.2)	70
9. Dokumentation	73
10. Häufige Mängel in der Praxis	74
II. Auslagerungs-, Weiterverlagerungs- und Konzentrationsrisiken	75
1. Auslagerungs- und Weiterverlagerungsrisiken	75
2. Konzentrationsrisiken	75
III. Durchführung regelmäßiger und anlassbezogener Risikoanalysen	77
1. Einleitung	77
2. Regelmäßige Überprüfung	77
3. Anlassbezogene Überprüfung	78
4. Übernahmen und Fusionen	78
5. Durchführung	78
IV. Ablauf einer Risikoanalyse in Anlehnung an den Risikoinventur-Prozess	81
1. Einleitung	81

2.	Vorbereitung	83
3.	Durchführung der Risikoanalyse	83
4.	Auswertung	84
5.	Dokumentation	84
V.	Einbindung maßgeblicher Organisationseinheiten	85
1.	Einleitung	85
2.	Beteiligte Organisationseinheiten und Funktionen	85
VI.	Überführung der Analyse-Ergebnisse in das Risikotragfähigkeitskonzept	88
D. Auslagerbarkeit von Kontroll- und Kernbankbereichen		93
I.	Neue MaRisk-Novelle als Impulsgeber	95
II.	Voraussetzungen für Auslagerung von Steuerungs- und Überwachungsbereichen	99
III.	Besondere Maßstäbe für Voll-/Teil-Auslagerung der Kontrollbereiche Risikocontrolling-, Compliance-Funktion und Interne Revision	101
1.	Compliance-Funktion im besonderen Fokus	101
2.	Besondere Kriterien auch für Risikocontrolling und die Interne Revision	104
IV.	Erleichterungen für kleinere Institute bei Vollauslagerung von Compliance und Revision	106
E. Aufbau einer Dienstleister-Steuerung		109
I.	Einführung	111
II.	IST-Analyse – Zusammentragen und Sichtung aller heutigen Dienstleisterverträge	113
1.	Anforderungen an Auslagerungsverträge	115
2.	Aktualität der Verträge – Schwerpunkt allgemeine Informationen	116
3.	Festlegungen von zukünftig zu überwachenden Verträgen	117

III. Zuständigkeiten und Verantwortliche	118
IV. Festlegung der Prozesse	120
V. Aufbau einer Risikoanalyse	124
VI. Berichtsauswertung – Bearbeitung der Informationspflichten des Dienstleisters	127
VII. Weiterverlagerung	131
VIII. Leistungsüberwachung – Anwendung von Service Level Agreements (SLA)	135
IX. Servicegespräche	138
X. Bericht an die Geschäftsführung	139
XI. Auswertung	140
XII. Zugriffsberechtigungen	141
XIII. Fazit	143
1. Dienstleister-Steuerung als Chance	143
2. Angemessene Personalbesetzung und Ausbildung	143
3. Vorstand als Sponsor	144
F. Handlungsoptionen und Notfallpläne bei Beendigung der Auslagerung	147
I. Vorbemerkungen	149
II. Vorkehrungen für beabsichtigte und erwartete Beendigung der Auslagerungsvereinbarung	152
1. Ursachen für beabsichtigte und erwartete Beendigungen von Auslagerungen	152
a) Entfall des externen Leistungsbedarfs bzw. »Insourcing«	152
b) Dauerhafte Schlechtleistung	153
c) Preiserhöhungen	154
d) Planmäßiger Anbieterwechsel	154
e) Erwartete Kündigung seitens des Dienstleisters	155

2.	Vorkehrungen und Handlungsoptionen im Falle des Eintritts beabsichtigter oder erwarteter Beendigungen von Auslagerungen	155
a)	Verzicht auf eine Leistung	155
b)	Eigenleistung (»Insourcing«)	156
c)	Alternative Anbieter durch Anbieterwechsel	156
d)	Mischformen z. B. durch Kooperationen	157
III.	Festlegung von Ausstiegsstrategien für die unbeabsichtigte oder unerwartete Beendigung von Auslagerungen	157
1.	Ursachen für unbeabsichtigte oder unerwartete Beendigungen von Auslagerungen	157
a)	Extern durch unerwartete Kündigung seitens des Dienstleisters	157
b)	Extern durch Ausfall des Dienstleisters, z. B. Insolvenz	158
2.	Ausstiegsstrategien	158
IV.	Handlungsoptionen in der Notfallplanung bei nicht festgelegten Ausstiegsstrategien	160
V.	Vereinbarung und Ausgestaltung von Kündigungsrechten für dauerhafte Schlechtleistung	162
1.	Überlegungen zur Vermeidung dauerhafter Schlechtleistungen	162
2.	Optionen zur Gewährleistung von Handlungsfähigkeiten im Falle dauerhafter Schlechtleistungen	163
a)	Allgemeine Vertragsklauseln	163
b)	Konkrete Vertragsklauseln	164
c)	Schadensersatzansprüche	165
3.	Anforderungen an ein effektives Vertragsmanagement	166
a)	Vertragsdaten	166
b)	IT-Unterstützung/Technik	169
c)	Prozesse	169
d)	Zusammenfassung	169

G. Berücksichtigung von Weiterverlagerungen im Auslagerungsvertrag	171
I. Vorüberlegungen zu Weiterverlagerungen	173
II. Vereinbarung von Zustimmungsvorbehalten zugunsten des auslagernden Instituts	178
III. Voraussetzungen für Weiterverlagerungen einzelner Arbeits- und Prozessschritte	181
IV. Sicherstellung und Anpassung der Berichtspflichten gegenüber auslagernden Instituten	183
V. Fazit	186
H. MaRisk-Compliance: Überwachung der Einhaltung vertraglicher, regulatorischer und gesetzlicher Anforderungen an Auslagerungen	189
I. Vorüberlegungen	191
II. Beurteilung der Einstufung der Wesentlichkeit von Auslagerungssachverhalten	191
1. Ausfallrisiken	195
2. Rechtsrisiken	196
3. Reputationsrisiken	197
4. Prozessrisiken	198
5. Sicherheitsrisiken	201
III. Zulässigkeit von Auslagerungen in Bezug auf Kontroll- und Kernbankbereiche	202
IV. Kontrolle der lfd. Leistungsüberwachung von Vertragsvereinbarungen (SLAs)	203
V. Überwachung des Reportings der Dienstleister-Steuerung und Auslagerungspartner	206
VI. Überwachung Exit Management: Kündigungsrechte, Ausstiegsstrategien, Notfallkonzepte	209

VII. Aufbau und Implementierung eines Dienstleister-Internes Kontrollsystems	212
VIII. Zusammenfassung und Ausblick	214
I. Plausibilitäts- und Prüfungspflichten der Internen Revision vor, während und nach der Auslagerung	215
I. Identifizierung von (nicht) wesentlichen Auslagerungen in der Prüflandkarte	217
1. Vorbemerkung	217
2. Evaluierung der vorliegenden Risikoanalysen	217
3. Festlegung des Prüfungsumfangs	219
4. Projektplanung und Einsatz von unterschiedlichen Prüfungsmethoden	219
a) Projektbegleitung und -prüfung	220
b) Wesentlichkeitseinstufung der Internen Revision	220
II. Beurteilung der Vergleichbarkeit einheitlicher Regelungen in Bezug auf Risikoanalysen	221
1. Festlegung von einheitlichen Beurteilungskriterien	221
2. Beurteilung der Schritte hin zum Netto-Risiko auf Plausibilität und Vollständigkeit	223
3. Begleitung der Internen Revision	226
III. Würdigung des zentralen Auslagerungsmanagements und Dienstleister-Reportings	227
1. Implementierung und Weiterentwicklung eines angemessenen Auslagerungsmanagements und entsprechender Kontroll- und Überwachungsprozesse	227
2. Erstellung und Pflege einer vollständigen Dokumentation der Auslagerungen (einschließlich Weiterverlagerungen)	229
3. Unterstützung der Fachbereiche bezüglich der institutsinternen und gesetzlichen Anforderungen bei Auslagerungen	231

4.	Koordination und Überprüfung der durch die zuständigen Bereiche durchgeführten Risikoanalyse gemäß AT 9 Tz. 2 der MaRisk	231
IV.	Vertragliche Festlegung von Informations- und Prüfungsrechten beim Dienstleister	233
1.	Vertragliche Ausgestaltung und aufsichtsrechtliche Anforderungen	233
2.	Informations- und Prüfungsrechte bei Weiterverlagerungen	235
3.	Vereinbarung von Weisungsrechten	235
V.	Eigene Analyse und Plausibilisierung der eingereichten Dienstleister-Prüfungsberichte	236
1.	Zeitnahe Analyse und Dokumentation der relevanten Dienstleister-Berichte	236
2.	Voraussetzungen für den Verzicht auf eigene Prüfungshandlungen	236
VI.	Veränderung in Prüffeldern und Aktualisierung von Prüf-Checklisten nach Auslagerung	239
1.	Notwendigkeit einer dynamischen Prüfungsplanung	239
2.	Continuous Auditing als Instrument der Risikofrüherkennung	239
J.	Bankaufsichtliche Überwachung von Auslagerungsprozessen	241
I.	Internes Kontrollsystem als maßgebliches Instrument	243
II.	Kapitalzuschläge wegen Mängeln bei Auslagerungen	244
III.	Auslagerungen als Schwerpunkt in Bankgeschäftlichen Prüfungen der Aufsicht	247
K.	Literaturverzeichnis	251
L.	Stichwortverzeichnis	255

A.

Einleitung

A. Einleitung¹

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 überprüfbareren 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 Schutzziele 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 Abgrenzungstatbestand²

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.

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

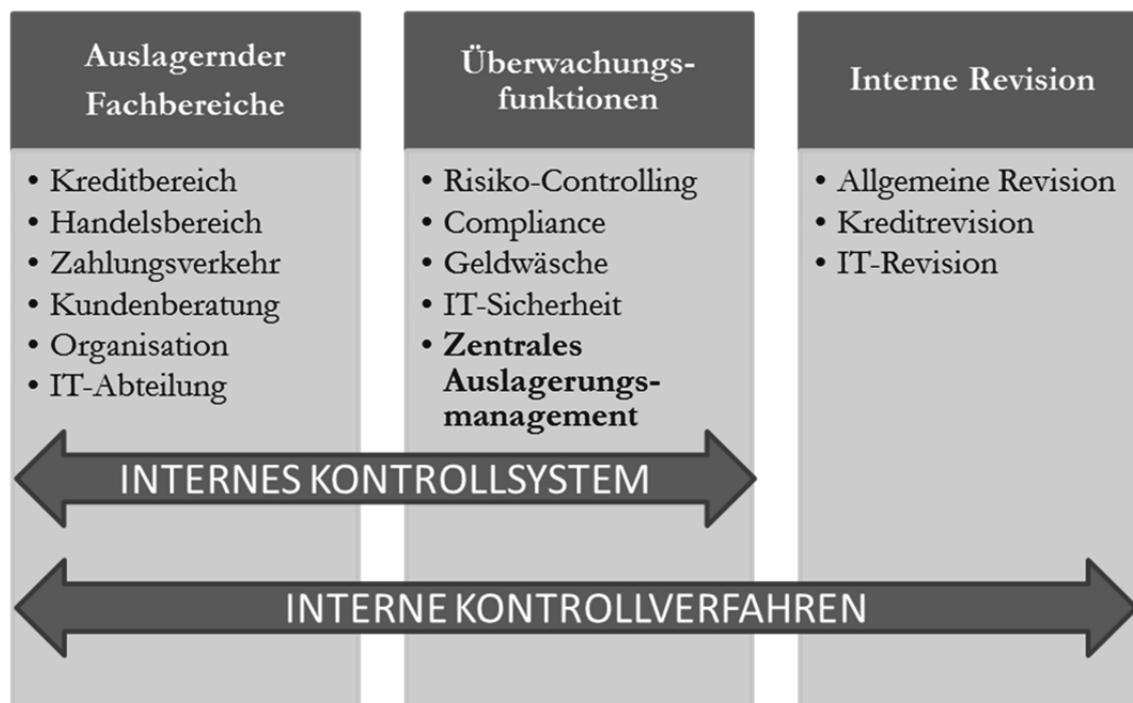


Abbildung B.1: Konzept der drei Verteidigungslinien bei Auslagerungen³

- 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. Beauftragungsfunktionen 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.