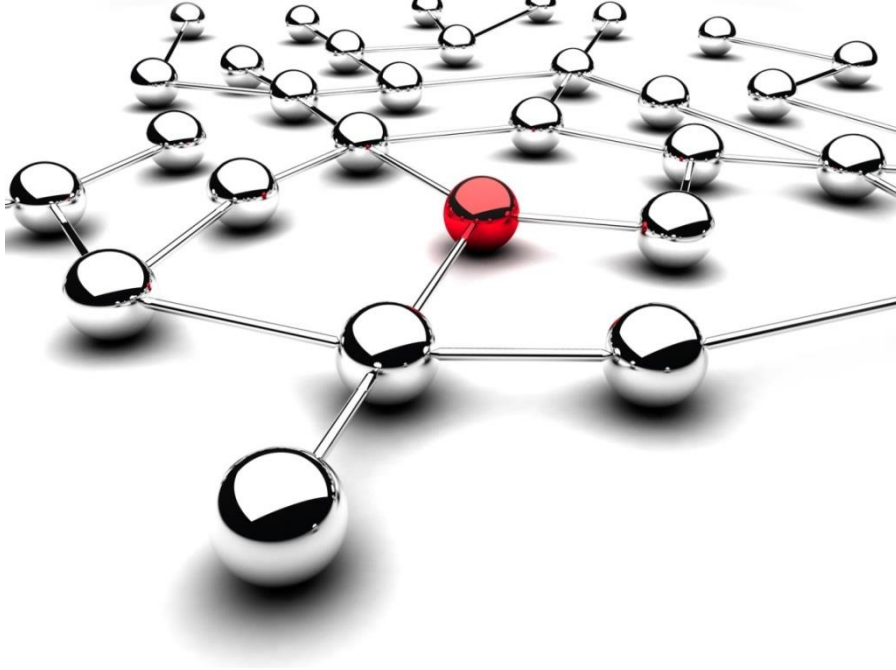
ISACA Germany Chapter

INNOVATION & TECH TALK ONLINE-EVENT



IT-COMPLIANCE IM RAHMEN DES AUSLAGERUNGSMANAGEMENTS AM BEISPIEL NEUER ANFORDERUNGEN FÜR FDL

JUNI 2021

compliance-net
partners for compliance and advisory

Referent

Ioannis Karamitros

- Geschäftsführer bei der compliance-net GmbH, eine Unternehmensberatung mit Sitz in Dreieich
- Seit 2005 als Revisor tätig und führt bis heute Prüfungen im IT und Non-IT Bereich für unterschiedliche Mandanten und im Auftrag von WPs in unterschiedlichen Branchen durch
- Schwerpunktmäßig als (IT-) Berater tätig im Bereich Umsetzung gesetzliche und aufsichtsrechtliche Anforderungen (z.B. BAIT, KAIT, Informationssicherheit), Weiterentwicklung Risikomanagementsysteme, Interne Kontrollsysteme und Themen wie Outsourcing in Banken, Versicherungen und Fintechs
- Unterstützung von Unternehmen bei der Vorbereitung von PS951 und ähnlichen Prüfungen
- Dozent an der dualen Hochschule Mannheim – Thema Risikomanagement in Versicherungsunternehmen
- Leitung ISACA Fachgruppe IT Compliance

Kontakt: Ioannis.Karamitros@compliance-net.com

compliance-net
partners for compliance and advisory

ISACA
Germany Chapter

Agenda

K1 Trend: Auslagerung IT

K2 Auslagerungsmanagementzyklus/-orga

K3

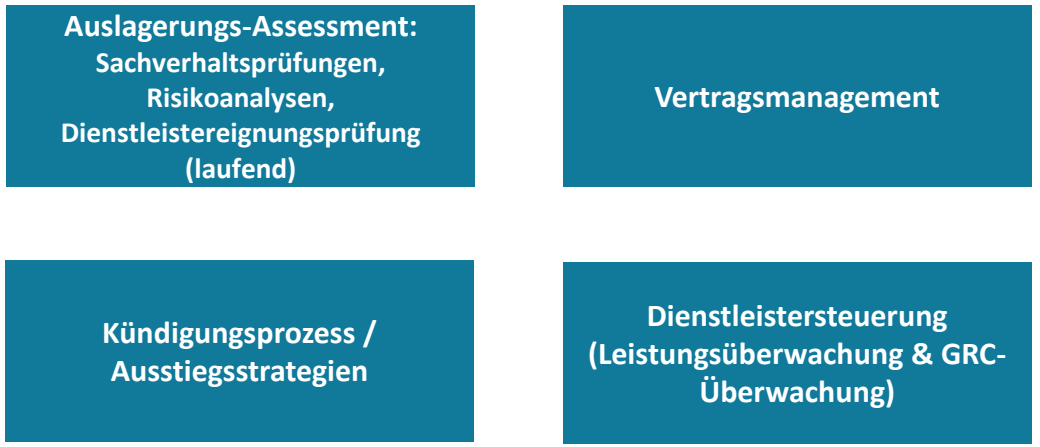
- Neue Anforderungen an das Auslagerungsmanagement
- Einfluss Auslagerungsmanagement auf IT-Compliance Status
- Hinweise aus der Praxis

1. Trend: Auslagerung IT

* an das Auslagerungsmanagement und an FDL an sich

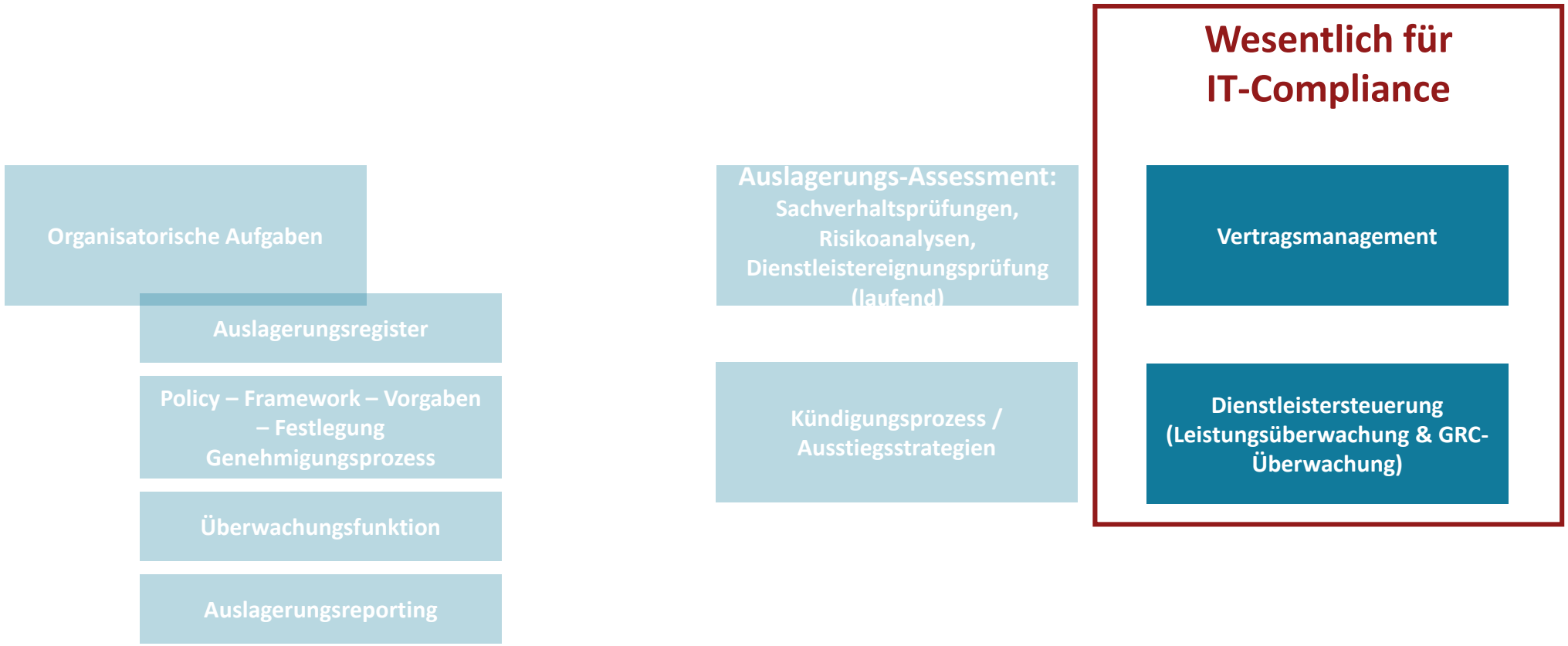
2. Auslagerungsmanagementzyklus/-orga

2nd Line



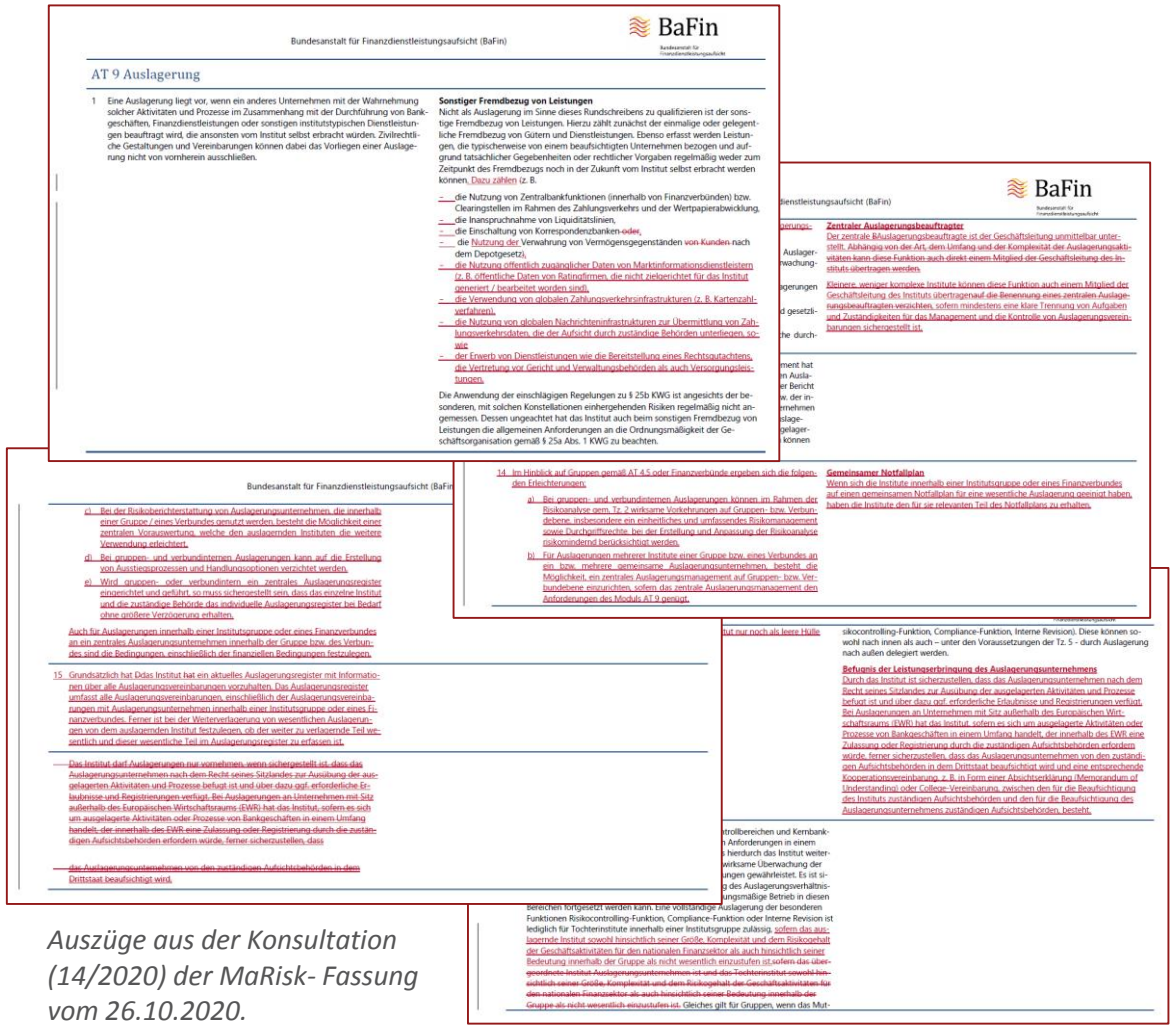
Wesentliche Phasen, umgesetzt i.d.R. durch 1st Line

2. Auslagerungsmanagementzyklus/-orga



Die „beste“ Organisation, die „beste“ Risikoanalyse und die durchdachtesten Ausstiegsprozesse reichen nicht aus, wenn der Dienstleister nicht überwacht wird und keine ordnungsgemäßen Verträge vorliegen.

3.1. Neue Anforderungen



Auszüge aus der Konsultation (14/2020) der MaRisk- Fassung vom 26.10.2020.

Der Entwurf der MaRisk-Konsultation sieht umfangreiche Anpassungen und Änderungen für Auslagerungsmanagement vor, insbesondere:

- Erhöhung Dokumentationspflichten – Register
- Erweiterung der Risikokriterien zur Einstufung von Dienstleistungen – umfangreiches Auslagerungs-Assessment
- Erweiterung der Vertragsinhalte für wesentliche Auslagerungen – Anpassungen von Verträgen
- Stärkerer Fokus auf Weiterverlagerungen (Sub-Dienstleister)
- Organisatorische Änderungen (ZAB, ZAM nicht unter Compliance-Funktion)
- Kriterien der Dienstleistersteuerung

compliance-net
partners for compliance and advisory

ISACA Germany Chapter

3.1. Neue Anforderungen

Weitere Rahmenbedingungen – BAIT

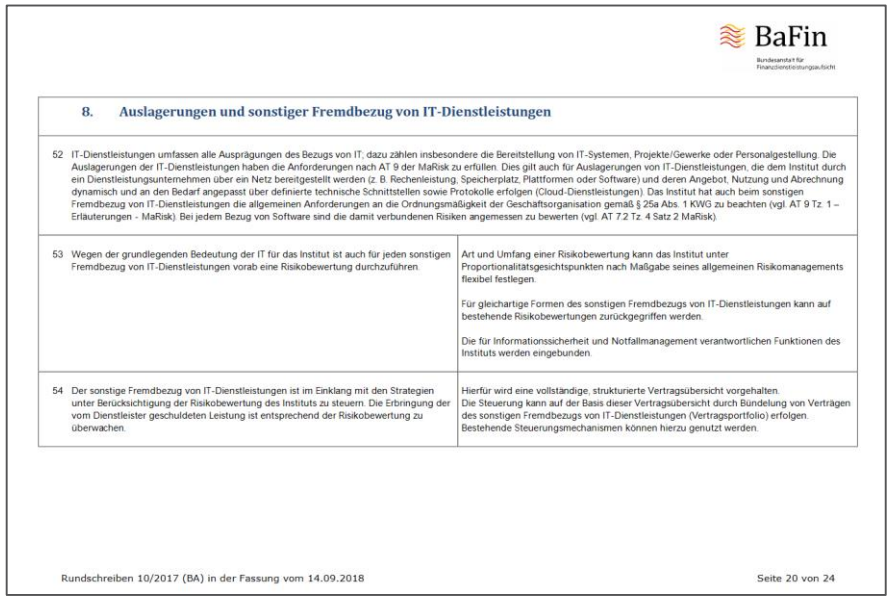
ACHTUNG BAIT NOVELLE KOMMT – Änderungen gering in Kapitel 8

BaFin
Bundesanstalt für Finanzdienstleistungsaufsicht

Rundschreiben 10/2017 (BA) in der Fassung vom 14.09.2018

An alle Kreditinstitute
und Finanzdienstleistungsinstitute
in der Bundesrepublik Deutschland

Bankaufsichtliche Anforderungen an die IT (BAIT)



BaFin
Bundesanstalt für Finanzdienstleistungsaufsicht

8. Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen

52	IT-Dienstleistungen umfassen alle Ausprägungen des Bezugs von IT; dazu zählen insbesondere die Bereitstellung von IT-Systemen, Projekte/Gewerke oder Personalgestellung. Die Auslagerungen der IT-Dienstleistungen haben die Anforderungen nach AT 9 der MaRisk zu erfüllen. Dies gilt auch für Auslagerungen von IT-Dienstleistungen, die dem Institut durch ein Dienstleistungsunternehmen über ein Netz bereitgestellt werden (z. B. Rechenleistung, Speicherplatz, Plattformen oder Software) und deren Angebot, Nutzung und Abrechnung dynamisch und an den Bedarf angepasst über definierte technische Schnittstellen sowie Protokolle erfolgen (Cloud-Dienstleistungen). Das Institut hat auch beim sonstigen Fremdbezug von IT-Dienstleistungen die allgemeinen Anforderungen an die Ordnungsmäßigkeit der Geschäftsorganisation gemäß § 25a Abs. 1 KWG zu beachten (vgl. AT 9 Tz. 1 – Erläuterungen - MaRisk). Bei jedem Bezug von Software sind die damit verbundenen Risiken angemessen zu bewerten (vgl. AT 7.2 Tz. 4 Satz 2 MaRisk).	
53	Wegen der grundlegenden Bedeutung der IT für das Institut ist auch für jeden sonstigen Fremdbezug von IT-Dienstleistungen vorab eine Risikobewertung durchzuführen.	Art und Umfang einer Risikobewertung kann das Institut unter Proportionalitätsgesichtspunkten nach Maßgabe seines allgemeinen Risikomanagements flexibel festlegen. Für gleichartige Formen des sonstigen Fremdbezugs von IT-Dienstleistungen kann auf bestehende Risikobewertungen zurückgegriffen werden. Die für Informationssicherheit und Notfallmanagement verantwortlichen Funktionen des Instituts werden eingebunden.
54	Der sonstige Fremdbezug von IT-Dienstleistungen ist im Einklang mit den Strategien unter Berücksichtigung der Risikobewertung des Instituts zu steuern. Die Erbringung der vom Dienstleister geschuldeten Leistung ist entsprechend der Risikobewertung zu überwachen.	Hierfür wird eine vollständige, strukturierte Vertragsübersicht vorgehalten. Die Steuerung kann auf der Basis dieser Vertragsübersicht durch Bündelung von Verträgen des sonstigen Fremdbezugs von IT-Dienstleistungen (Vertragsportfolio) erfolgen. Bestehende Steuerungsmechanismen können hierzu genutzt werden.

Rundschreiben 10/2017 (BA) in der Fassung vom 14.09.2018 Seite 20 von 24

3.2. Auslagerungsregister

Ein Auslagerungsregister wird in AT 9 Ziffer 15 explizit gefordert:

- Umfangreiche Informationen über Auslagerungsvereinbarungen inkl. der internen Auslagerungen sowie wesentliche Teile bei Weiterverlagerung.
- Hinweis aus der Praxis für den Aufbau: siehe EBA GL/2019/02 Kapitel 11 – die MaRisk ist sehr allgemein in der Fomulierung

U.a. auch:
- Angaben zu den Überwachungsmaßnahmen und Risikoanalysen
- Vertragsinformationen
- Referenznummern
- Informationen zu Subdienstleistern
- Cloud-Nutzung
- Standorte der Datenverarbeitung

3.3. Auslagerungs-Assessment




1

Prüfung Sachverhalt
Neuerung bei der Einstufung AT 9 Ziffer 1:
Kriterien für **Sonstiger Fremdbezug**

2

Prüfung Auslagerbarkeit
Keine wesentlichen Neuerungen oder Änderungen (vgl. z.B. AT 9 Ziffer 5)

3

Risikoanalyse und Wesentlichkeitsprüfung
(inkl. Dienstleistereignung)
AT.9 Ziffer 2
Erweiterung der Risikokriterien

Neuerung in AT 9 Ziffer 11:
Risiken aus Weiterverlagerungsketten

Ergebnis Auslagerungs-Assessment

3.4. Vertragsmanagement

„Einkauf“ von Dienstleistungen
(Vertragsbestandteile)

AT 9 Ziffer 7 sieht erweiterte Vertragsklauseln für wesentliche Auslagerungen vor:

- Umfassendere Informations- und Prüfungsrechte – Geltung **auch für nicht-wesentliche** Auslagerungen (falls absehbar, dass sich die Kategorisierung ändert)
- Kündigungsrechte – Verpflichtung des Dienstleisters zur Unterstützung bei der Re-Integration oder Übertragung der Auslagerung nach Kündigung
- …

Wesentlich für IT-Compliance

Vertragsmanagement

compliance-net
partners for compliance and advisory

ISACA Germany Chapter

3.4. Vertragsmanagement

„Einkauf“ von Dienstleistungen
(Vertragsbestandteile)

Typische Versäumnisse

- (Insbesondere ältere) Verträge werden nicht um neue Anforderungen an de IT ergänzt – z.B. PSD2 Anforderungen (kommen u.a. jetzt über BAIT 2.0)
- Rahmenverträge sind zu allgemein gestaltet
- Prüfungsrechte und Umgang mit Sub-Dienstleistern nicht hinreichend geregelt
- Dienstleister hat selbst keine guten Verträge mit seinen Dienstleistern

Wesentlich für IT-Compliance

Vertragsmanagement

3.6. Dienstleistersteuerung – Arten

Dienstleistersteuerung

Ziel: Steuerung der Risiken / Überwachung

Gilt auch für interne Auslagerungssachverhalte

- Business Controlling / Leistungsüberprüfung
  - Bei wesentlichen Auslagerungen Messkriterien
  - Überwachung Einhaltung SLAs
  - Prüfung Rechnungsstellung
- Überwachung GRC / IT-Umfeld / Schwerpunkt: ITGC

Wesentlich für IT-Compliance

Dienstleistersteuerung (Leistungsüberwachung & GRC-Überwachung)

3.6. Dienstleistersteuerung – Organisation

Dienstleistersteuerung

Ziel: Steuerung der Risiken / Überwachung

Gilt auch für interne Auslagerungssachverhalte

- Auslagernde Organisationseinheit überwacht den Dienstleister (Kernproblem: Fachbereiche sollen IT Sachverhalte beurteilen)
- Überwachung der Organisationseinheit durch das Auslagerungsmanagement
  - Umsetzung der Vorgaben für Dienstleistersteuerung durch Organisationseinheiten
- Revision -> Prüfung der Dienstleister bei Bedarf und Prüfung des Dienstleistersteuerungsprozesses

Wesentlich für IT-Compliance

Dienstleistersteuerung (Leistungsüberwachung & GRC-Überwachung)

3.6. Dienstleistersteuerung – Nachweise GRC

- PS951 / ISAE 3402 und sonstige von externen WP etc. ausgestellten Nachweisen
- (Externe) Revisionsberichte, sofern Revision MaRisk konform aufgestellt ist, sich an den beruflichen Standards orientiert
- Eigene Besichtigungen, „Walk-Throughs“
- Eigene Revision prüft Dienstleister
- Vorsicht bei Berichten, ausgestellt durch Dienstleister selbst -> dennoch verwertbar: DSB-Berichte, ISB-Berichte, BCM-Berichte
- Vorsicht bei ISO-Zertifikaten

In der Regel jährliche Überprüfung

Wesentlich für IT-Compliance

Dienstleistersteuerung (Leistungsüberwachung & GRC-Überwachung)

3.6. Dienstleistersteuerung – Business Controlling

- Regelmäßige Meetings / Austausch über Dienstleistungen, Status und Entwicklung
- Regelmäßige Überwachung von Kennzahlen
- Regelmäßige Überwachung Einhaltung SLAs
- Regelmäßige Überprüfung Rechnungsstellungen durch Dienstleister
- Änderungen in der Struktur / Organisation des Dienstleisters / Sub-Dienstleister (wenn ja, dann auch GRC beachten und Auslagerungsassessment überprüfen

Wesentlich für IT-Compliance

Dienstleistersteuerung (Leistungsüberwachung & GRC-Überwachung)

3.6. Dienstleistersteuerung – Sub-Dienstleister

- Voraussetzung: Über die komplette Auslagerungskette liegen „MaRisk konforme“ Verträge vor
- Dienstleister hat den Sub-Dienstleister nach gleichen Maßstäben zu überprüfen, Berichte sind vorzulegen
- Anwendung der Prüfungsrechte bei entsprechenden Verträgen -> Auslagerndes Unternehmen prüft Sub-Dienstleister direkt

Wesentlich für IT-Compliance

Dienstleistersteuerung (Leistungsüberwachung & GRC-Überwachung)

3.6. Dienstleistersteuerung – Typische Fehler

- „Blindes Vertrauen“ in Dienstleister – „deswegen lagern wir ja aus, das muss schon funktionieren“
- Sub-Dienstleister werden nicht in die Überwachung einbezogen
- Experten werden seitens der dezentralen Auslagerungskoordinatoren nicht eingebunden -> fehlerhafte Rückschlüsse – Fachbereiche und IT müssen zusammenarbeiten
- „Falsche“ Berichte eingeholt
- Unvollständige Einholung von Nachweise -> Verlass auf Dokumente mit wenig Beweiskraft
- Interne Revision des Dienstleisters ist evtl. nicht MaRisk-konform
- Ergebnisse der Dienstleistersteuerung werden nicht in das Auslagerungsassessment eingebunden → fehlerhafte Rückschlüsse für den IT-Compliance Status

Wesentlich für IT-Compliance

Dienstleistersteuerung (Leistungsüberwachung & GRC-Überwachung)

VIELEN DANK

Sie haben weitere Fragen? Wenden Sie sich gerne an uns:

Ioannis.Karamitros@compliance-net.com oder fg-it-compliance@isaca.de

Mobil: 0170-2180916

ISACA Germany Chapter

compliance-net
Partners for compliance and advisory

compliance-net akademie
Robert-Bosch-Str. 32
63303 Dreieich
Webseite: www.compliance-net-akademie.de
Fachseite: www.compliance-net.de