

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

JUNI 2021

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

Agenda

K1 Trend: Auslagerung IT

K2 Auslagerungsmanagementzyklus/-orga

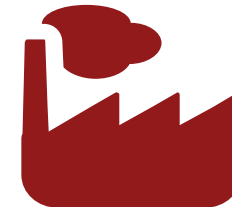
- K3**
- Neue Anforderungen an das Auslagerungsmanagement
 - Einfluss Auslagerungsmanagement auf IT-Compliance Status
 - Hinweise aus der Praxis

1. Trend: Auslagerung IT

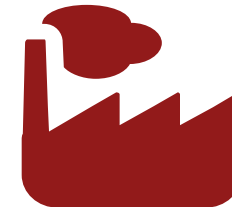


* an das Auslagerungsmanagement und an FDL an sich

Verstärkt Auslagerung der IT (intern und extern)



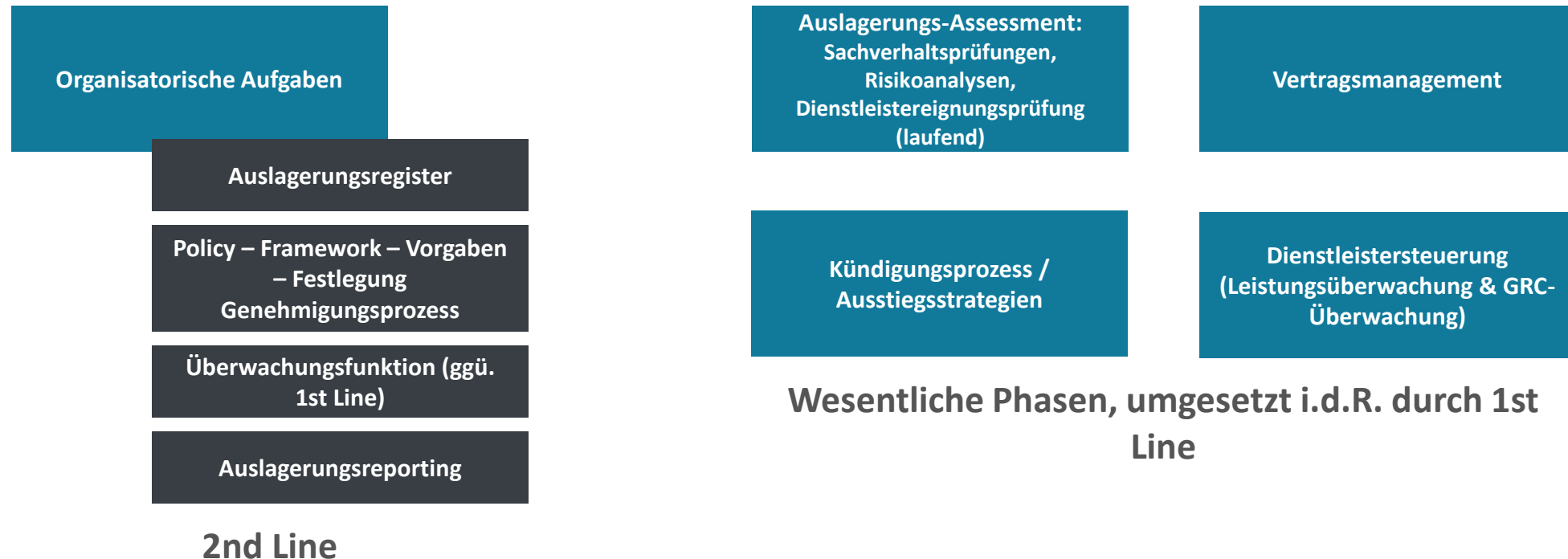
IT-Dienstleister



Sub-Dienstleister

Starker Einfluss auf den IT-Compliance Status des auslagernden Unternehmens

2. Auslagerungsmanagementzyklus/-orga



2. Auslagerungsmanagementzyklus/-orga



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

3.1. Neue Anforderungen

<p>Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)</p> <p>AT 9 Auslagerung</p> <p>1. Eine Auslagerung liegt vor, wenn ein anderes Unternehmen mit der Wahrnehmung solcher Aktivitäten und Prozesse im Zusammenhang mit der Durchführung von Bankgeschäften, Finanzdienstleistungen oder sonstigen institutstypischen Dienstleistungen beauftragt wird, die ansonsten vom Institut selbst erbracht würden. Zweckliche Gestaltungen und Vereinbarungen können dabei das Vorliegen einer Auslagerung nicht von vornherein ausschließen.</p> <p>Sonstiger Fremdbezug von Leistungen Nicht als Auslagerung im Sinne dieses Rundschreibens zu qualifizieren ist der sonstige Fremdbezug von Leistungen. Hierzu zählt zunächst der einmalige oder gelegentliche Fremdbezug von Gütern und Dienstleistungen. Ebenso erfasst werden Leistungen, die typischerweise von einem beauftragten Unternehmen bezogen und aufgrund tatsächlicher Gegebenheiten oder rechtlicher Vorgaben regelmäßig weiter zum Zeitpunkt des Fremdbezugs noch in der Zukunft vom Institut selbst erbracht werden können. Dazu zählen (z. B.</p> <ul style="list-style-type: none"> – die Nutzung von Zentralbankfunktionen (innerhalb von Finanzverbänden) bzw. Clearingstellen im Rahmen des Zahlungsverkehrs und der Wertpapierabwicklung, – die Inanspruchnahme von Liquiditätslinien, – die Einschaltung von Korrespondenzbanken oder, – die Nutzung der Verwahrung von Vermögensgegenständen von Kunden nach dem Depotgesetz, – die Nutzung öffentlich zugänglicher Daten von Marktinformationsdienstleistern (z. B. öffentliche Daten von Ratingfirmen, die nicht zielgerichtet für das Institut angesetzt / beauftragt worden sind), – die Verwendung von abgebauten Zahlungsverkehrsinfrastrukturen (z. B. Kartenzahlverfahren), – die Nutzung von abgebauten Nachrichteninfrastrukturen zur Übermittlung von Zahlungsvorschriften, die der Aufsicht durch zuständige Behörden unterliegen, sowie – der Erwerb von Dienstleistungen wie die Bereitstellung eines Rechtsfachdienstes, die Vertretung vor Gericht und Verwaltungsbehörden als auch Versorgungsleistungen. <p>Die Anwendung der einschlägigen Regelungen zu § 25a KWG ist angesichts der besonderen, mit solchen Konstellationen einhergehenden Risiken regelmäßig nicht angemessen. Dessen ungeachtet hat das Institut auch beim sonstigen Fremdbezug von Leistungen die allgemeinen Anforderungen an die Ordnungsmäßigkeit der Geschäftsorganisation gemäß § 25a Abs. 1 KWG zu beachten.</p>	<p>BaFin</p> <p>Dienstleistungsaufsicht (BaFin)</p> <p>Zentraler Auslagerungsbeauftragter Der zentrale Auslagerungsbeauftragte ist der Geschäftsführung unmittelbar unterstellt, abhängig von der Art, dem Umfang und der Komplexität der Auslagerungstätigkeiten kann diese Funktion auch direkt einem Mitglied der Geschäftsführung des Instituts übertragen werden.</p> <p>Kleinere, weniger komplexe Institute können diese Funktion auch einem Mitglied der Geschäftsführung des Instituts übertragen auf die Benennung eines zentralen Auslagerungsbeauftragten verzichten, sofern mindestens eine klare Trennung von Aufgaben und Zuständigkeiten für das Management und die Kontrolle von Auslagerungsleistungen sichergestellt ist.</p> <p>meet hat in Ausla- bericht der er- mehren slage- belegen können</p>
<p>Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)</p> <p>14. Im Hinblick auf Gruppen gemäß AT 4.5 oder Finanzverbände ergeben sich die folgenden Erleichterungen:</p> <p>a) Bei gruppen- und verbandsinternen Auslagerungen können im Rahmen der Risikoprüfung gem. Tz. 2.2.3.3 weitere Vorkehrungen auf Gruppen- bzw. Verbands-ebene, insbesondere ein einheitliches und umfassendes Risikomanagement sowie Durchgriffrechte bei der Erstellung und Anpassung der Risikoanalyse risikoorientiert berücksichtigt werden.</p> <p>b) Für Auslagerungen mehrerer Institute einer Gruppe bzw. eines Verbandes an ein bzw. mehrere gemeinsame Auslagerungsunternehmen besteht die Möglichkeit ein zentrales Auslagerungsmanagement auf Gruppen- bzw. Verbandsebene einzurichten, sofern das zentrale Auslagerungsmanagement den Anforderungen des Moduls AT 9 genügt.</p> <p>Gemeinsamer Notfallplan Wenn sich die Institute innerhalb einer Institutengruppe oder eines Finanzverbundes auf einem gemeinsamen Notfallplan für eine wesentliche Auslagerung einigen haben, haben die Institute dies für sie relevanten Teil des Notfallplans zu erhalten.</p> <p>Integrieren und Kernbank-Anforderungen in einem Hierdurch das Institut weiter- wirkbare Überwachung der- ingen gewährleistet. Es ist so- ge des Auslagerungsverhaltens- gemäßige Betrieb in diesen</p>	<p>BaFin</p> <p>Integrieren und Kernbank-Anforderungen in einem Hierdurch das Institut weiter- wirkbare Überwachung der- ingen gewährleistet. Es ist so- ge des Auslagerungsverhaltens- gemäßige Betrieb in diesen</p>
<p>15. Grundsätzlich hat das Institut bei einem aktuellen Auslagerungsregister mit Informationen über alle Auslagerungsverhältnisse vorzuhalten. Das Auslagerungsregister umfasst alle Auslagerungsverhältnisse einschließlich der Auslagerungsvereinbarungen mit Auslagerungsunternehmen innerhalb einer Institutengruppe oder eines Finanzverbundes. Ferner ist bei der Weiterentwicklung von wesentlichen Auslagerungen von dem auslagernden Institut zu klären, ob die weiter zu verändernde Teil essenziell und dieser wesentliche Teil ein Auslagerungsregister zu erfassen ist.</p> <p>Auch für Auslagerungen innerhalb einer Institutengruppe oder eines Finanzverbundes an ein zentrales Auslagerungsunternehmen innerhalb der Gruppe bzw. des Verbandes sind die Bestimmungen, einschließlich der finanziellen Bedingungen festzulegen.</p> <p>Das Institut darf Auslagerungen nur vornehmen, wenn sichergestellt ist, dass das Auslagerungsunternehmen nach dem Recht seines Sitzlandes zur Ausübung der ausgelagerten Aktivitäten und Prozesse befähigt ist und über dazu aus- reifende Er- fahrung und Ressourcen verfügt. Bei Auslagerungen an Institute mit Sitz außerhalb des Europäischen Wirtschaftsraums (EWR) hat das Institut, sofern es sich um ausgelagerte Aktivitäten oder Prozesse von Bankgeschäften in einem Umfang handelt, die innerhalb des EWR eine Zulassung oder Registrierung durch die zustän- digen Aufsichtsbehörden erfordern würde, ferner sicherzustellen, dass</p> <p>Das Auslagerungsunternehmen von den zuständigen Aufsichtsbehörden in dem Drittstaat beauftragt wird.</p>	<p>Integrieren und Kernbank-Anforderungen in einem Hierdurch das Institut weiter- wirkbare Überwachung der- ingen gewährleistet. Es ist so- ge des Auslagerungsverhaltens- gemäßige Betrieb in diesen</p> <p>Reifens der Leistungsreife des Auslagerungsunternehmens Durch das Institut ist sicherzustellen, dass das Auslagerungsunternehmen nach dem Recht seines Sitzlandes zur Ausübung der ausgelagerten Aktivitäten und Prozesse befähigt ist und über dazu aus- reifende Er- fahrung und Ressourcen verfügt. Bei Auslagerungen an Internationales mit Sitz außerhalb des Europäischen Wirtschaftsraums (EWR) hat das Institut, sofern es sich um ausgelagerte Aktivitäten oder Prozesse von Bankgeschäften in einem Umfang handelt, die innerhalb des EWR eine Zulassung oder Registrierung durch die zuständigen Aufsichtsbehörden erfordern würde, ferner sicherzustellen, dass das Auslagerungsunternehmen von den zustän- digen Aufsichtsbehörden in dem Drittstaat beauftragt wird und eine entsprechende Kooperationsvereinbarung, z. B. in Form einer Absichtserklärung (Memorandum of Understanding) oder Colloc- Vereinbarung, zwischen den für die Beaufichtigung des Instituts zuständigen Aufsichtsbehörden und den für die Beaufichtigung des Auslagerungsunternehmens zuständigen Aufsichtsbehörden, besteht.</p> <p>Integrieren und Kernbank-Anforderungen in einem Hierdurch das Institut weiter- wirkbare Überwachung der- ingen gewährleistet. Es ist so- ge des Auslagerungsverhaltens- gemäßige Betrieb in diesen</p> <p>Reifens der Leistungsreife des Auslagerungsunternehmens Durch das Institut ist sicherzustellen, dass das Auslagerungsunternehmen nach dem Recht seines Sitzlandes zur Ausübung der ausgelagerten Aktivitäten und Prozesse befähigt ist und über dazu aus- reifende Er- fahrung und Ressourcen verfügt. Bei Auslagerungen an Internationales mit Sitz außerhalb des Europäischen Wirtschaftsraums (EWR) hat das Institut, sofern es sich um ausgelagerte Aktivitäten oder Prozesse von Bankgeschäften in einem Umfang handelt, die innerhalb des EWR eine Zulassung oder Registrierung durch die zuständigen Aufsichtsbehörden erfordern würde, ferner sicherzustellen, dass das Auslagerungsunternehmen von den zustän- digen Aufsichtsbehörden in dem Drittstaat beauftragt wird und eine entsprechende Kooperationsvereinbarung, z. B. in Form einer Absichtserklärung (Memorandum of Understanding) oder Colloc- Vereinbarung, zwischen den für die Beaufichtigung des Instituts zuständigen Aufsichtsbehörden und den für die Beaufichtigung des Auslagerungsunternehmens zuständigen Aufsichtsbehörden, besteht.</p>

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

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

3.1. Neue Anforderungen

Weitere Rahmenbedingungen – BAIT

**ACHTUNG BAIT –
NOVELLE KOMMT –
Änderungen gering in
Kapitel 8**



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)



8. Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen

<p>52 IT-Dienstleistungen umfassen alle Ausprägungen des Bezugs von IT, dazu zählen insbesondere die Bereitstellung von IT-Systemen, Projekte/Gewerke oder Personalstellung. 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).</p>	
<p>53 Wegen der grundlegenden Bedeutung der IT für das Institut ist auch für jeden sonstigen Fremdbezug von IT-Dienstleistungen vorab eine Risikobewertung durchzuführen.</p>	<p>Art und Umfang einer Risikobewertung kann das Institut unter Proportionalitätsgesichtspunkten nach Maßgabe seines allgemeinen Risikomanagements flexibel festlegen.</p> <p>Für gleichartige Formen des sonstigen Fremdbezugs von IT-Dienstleistungen kann auf bestehende Risikobewertungen zurückgegriffen werden.</p> <p>Die für Informationssicherheit und Notfallmanagement verantwortlichen Funktionen des Instituts werden eingebunden.</p>
<p>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.</p>	<p>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.</p>

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 Formulierung

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

3.4. Vertragsmanagement

„Einkauf“ von Dienstleistungen
(Vertragsbestandteile)



Typische Versäumnisse

- (Insbesondere ältere) Verträge werden nicht um neue Anforderungen an die 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 Auslagerungskordinatoren 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



compliance-net akademie

Robert-Bosch-Str. 32

63303 Dreieich

Webseite: www.compliance-net-akademie.de

Fachseite: www.compliance-net.de
