Deloitte.

Strategisches Outsourcing Management – Herausforderungen in der Gestaltung und regulatorischen Praxis

Thomas John

Deloitte Audit Wirtschaftsprüfungs GmbH

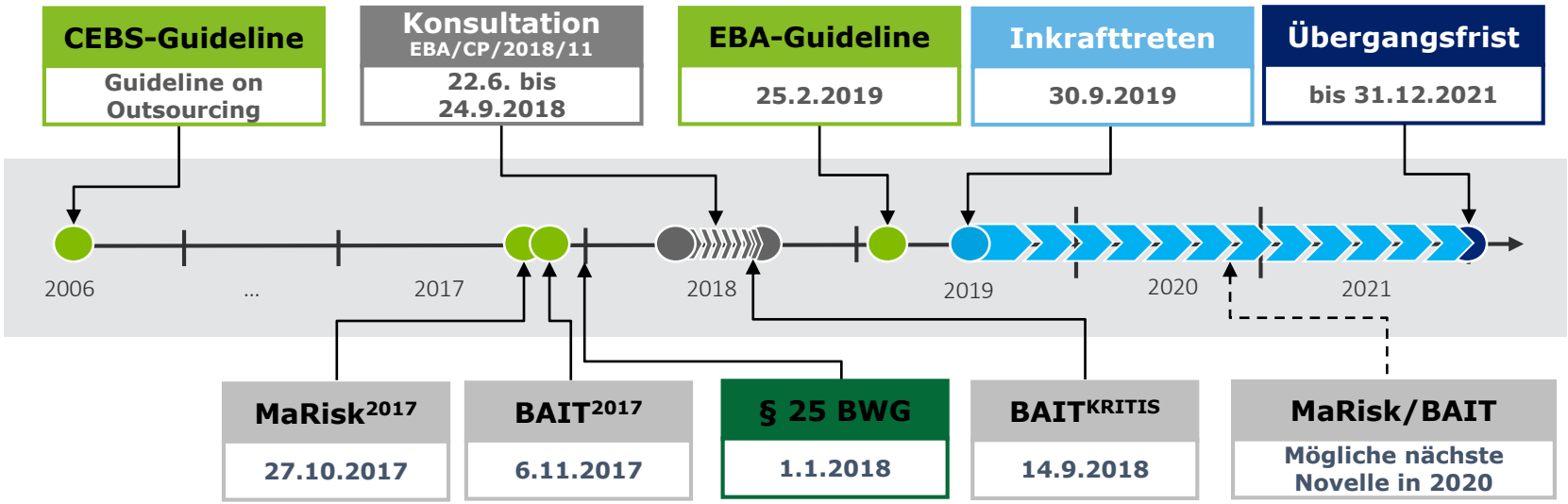
Wien, 7. Juli 2020

Agenda

1. **Pflichten und Anforderungen im Lebenszyklus eines Outsourcings**
2. **Wie überwache und steuere ich einen Dienstleister?**
3. **Erfahrungen zur regulatorischen Praxis in Österreich und Deutschland**

Leitlinien zu Auslagerungsvereinbarungen (EBA/GL/2019/02)

Umsetzungsstatus und nächste Schritte



- Veröffentlichung des Konsultationspapiers am 22. Juni 2018; Konsultationsphase bis 24. September 2018; öffentliche Anhörung am 4. September 2018.
- Die überarbeiteten **Leitlinien wurden am 25. Februar 2019 veröffentlicht** und traten am **30. September 2019 in Kraft**. Insbesondere neue Auslagerungsvereinbarungen sind dann gem. der überarbeiteten Leitlinie abzuschließen.
- Für die Anpassung der Auslagerungsverträge bestehender Auslagerungen (mit Ausnahme von Auslagerungen an Cloud Dienstleister) sowie eine entsprechende Dokumentation läuft die **Umsetzungsfrist bis zum 31. Dezember 2021**.

Leitlinien zu Auslagerungsvereinbarungen (EBA/GL/2019/02)

Überblick – wesentliche Neuerungen bzw. Konkretisierungen

- Pre-Outsourcing-Phase beinhaltet eine umfangreiche Due Diligence und Risiko-bewertung inkl. Mitigationsüberlegungen, sowie Beurteilung von Interessenkonflikten
- Überwachung und Steuerung (inkl. regelmäßigem Update der Risikoanalyse) grds. für alle Auslagerungen nötig
- Einrichtung **Outsourcing-Datenbank** mit granularen Informationen auf Instituts-/ Gruppenebene
- Neue **Informationspflichten** gegenüber der Aufsicht

- CRR-Kreditinstitute, CRR-Wertpapierfirmen sowie Zahlungs- und E-Geld-Institute
- Einhaltung auf **Einzel- und Gruppenebene**

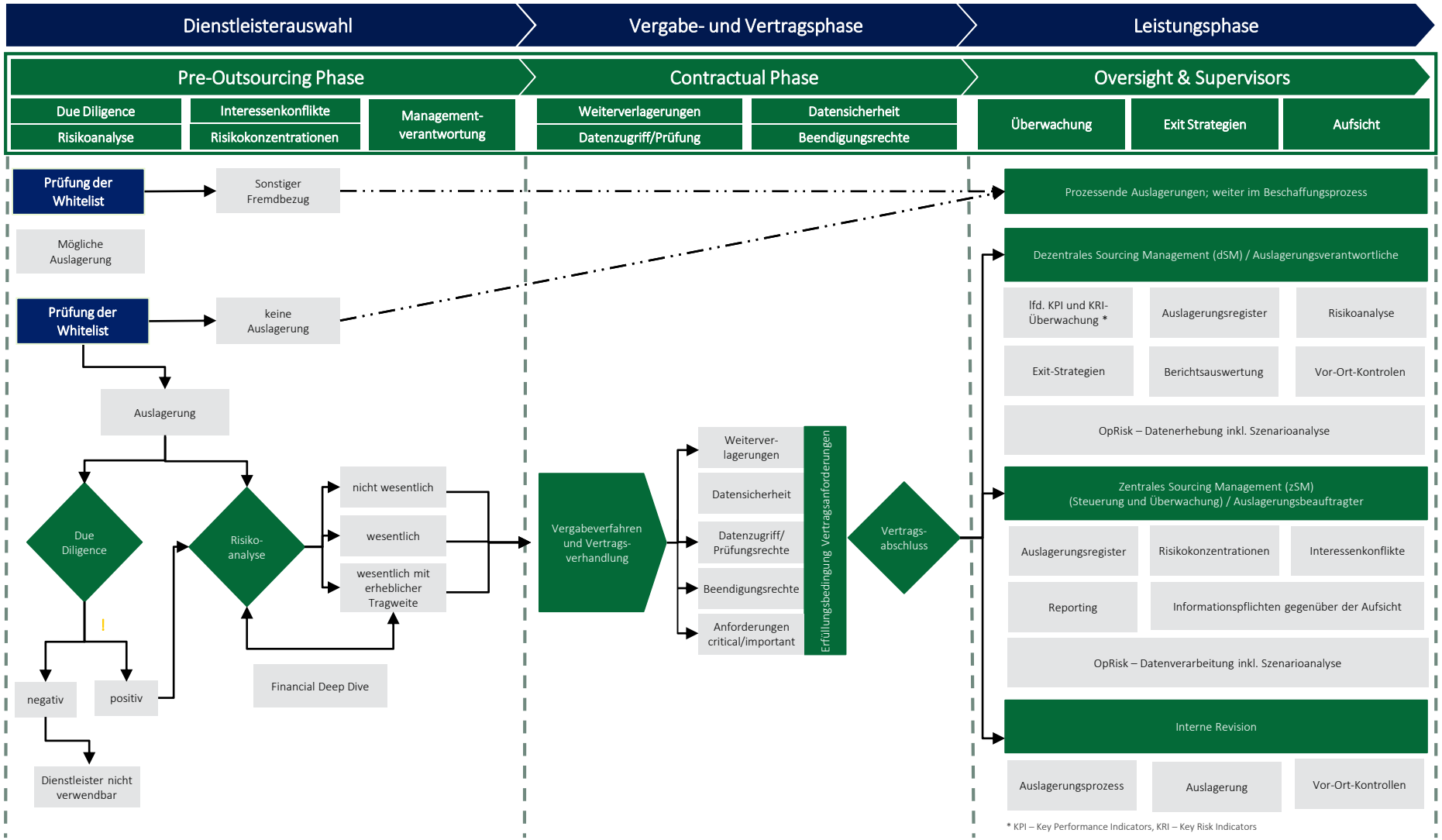
- **Vorgelagerte Beurteilung** der Outsourcing-Vereinbarungen unter Berücksichtigung der Definition „critical or important“
- Vertragliche Anforderungen gelten grds. für alle Auslagerungen (MaRisk-Vertragsanforderungen gelten bisher nur für wesentliche Auslagerungen)
- **Zusätzliche Vertragsregelungen** für als „critical or important“ eingestufte Auslagerungen

- Analyse der **Informationsschutzziele** der Auslagerung und Prüfung der Umsetzbarkeit dieser Ziele beim Dienstleister
- Pflicht einer angemessenen Information der Aufsichtsbehörden über Cloud-Auslagerungsvorhaben
- Regelungen zur Kontrolle für Einhaltung von Sicherheitsstandards und Durchführung von **IT-Sicherheitspenetrationstests**

- Einrichtung Outsourcing-Funktion
- Outsourcing-Policy mit vorgegebenen Mindestinhalten (Institut und Gruppe)
- **Untersuchung Interessenskonflikte**
- Einbindung Auslagerungsprozesse in Notfallplanung

Leitlinien zu Auslagerungsvereinbarungen (EBA/GL/2019/02)

Pflichten und Anforderungen im Lebenszyklus einer Auslagerung



Risikomanagement und Dienstleistersteuerung im Three-Lines of Defense Modell

Aufgaben der 1st Line (dezentrales Sourcing Management)

Erstellung der Risikoanalyse* (Initial, regelmäßig und anlassbezogen)

KPI und Service Level Definition

- Die ausgelagerten Dienstleistungen sind nach einem risikobasierten Ansatz zu überwachen (Tz. 100)
- Sicherstellung, dass die ausgelagerte Dienstleistung den institutsinternen Leistungs- und Qualitätsstandards entspricht → Vereinbarung von Service-Levels mit dem Dienstleister (Tz. 104)
- Definition von Leistungsindikatoren (z.B. Kontrollindikatoren und Risikoindikatoren) zur Leistungsmessung (Tz. 104 lit. b)

Operative Dienstleister-überwachung

- Überprüfung der Einhaltung der vereinbarten Service-Levels anhand der definierten Leistungsindikatoren (Tz. 104)
- Überprüfung kann anhand von Berichten erfolgen, die der Dienstleister selbst erstellt hat oder durch Dritte (z.B. Wirtschaftsprüfungsgesellschaften) erstellt wurden (Tz. 104)
- Bei wesentlichen Auslagerungen ist sicherzustellen, dass die Berichte qualitativ und quantitativ angemessen sind (Tz. 91 lit. b i.V.m. Tz. 92 und Tz. 93)

Vor-Ort-Kontrollen

- Institute sollten ihre Zugangs- und Prüfungsrechte anhand eines risikobasierten Ansatz ausüben (Tz. 90)
- Bei wesentlichen Auslagerungen dürfen sich die Institute nicht ausschließlich und dauerhaft auf die Auswertung von Berichten verlassen (Tz. 92)
- Vor-Ort-Prüfungen sind somit regelmäßig durch die Interne Revision (Tz. 85) oder durch das dezentrale Sourcing Management durchzuführen

Maßnahmenpläne, Eskalations-prozesse

- Maßnahmendefinition inkl. Eskalationsprozesse (Tz. 105):
- Sofern Mängel bei der Erbringung der ausgelagerten Funktion festgestellt werden, sind durch das Institut geeignete Maßnahmen zu ergreifen
- Es sind Eskalationsprozesse für den Fall zu implementieren, dass die vereinbarten Maßnahmen nicht durch den Dienstleister umgesetzt werden
- Der Eskalationsprozess kann die fristlose Kündigung und damit die Einleitung des Exits zur Folge haben

Pflege der auslagerungsbezogenen Daten ins Auslagerungsregister

NFR-Datenerhebung für die OpRisk-Steuerung inkl. Szenarioanalyse

* inkl. Weiterverlagerungen

Risikomanagement und Dienstleistersteuerung im Three-Lines of Defense Modell

Aufgaben der 2nd Line (zentrales Sourcing Management)

Abnahme der Risikoanalyse* (Initial, regelmäßig und anlassbezogen)

Risiko-konzentrationen

- Ermittlung kann in einem zweistufigen Verfahren erfolgen (Tz. 31 lit. e, Tz. 66 lit a, b & Tz. 103):
  - 1. Stufe: Erhebung der Risikokonzentrationen im Rahmen der Risikoanalyse von dem dSM
  - 2. Stufe: Validierung und Vervollständigung der Ergebnisse der 1. Stufe durch das zSM über das Auslagerungsregister sowie Wesentlichkeitsbewertung und Beurteilung der Auswirkungen auf die Risikosituation

Interessens-konflikte

- Konzipierung eines zweistufigen Prozesses zur Identifizierung, Bewertung und Steuerung von Interessenskonflikten (Tz. 45 bis 48)
  - 1. Stufe: Identifizierung und Bewertung von Interessenskonflikten innerhalb der Risikoanalyse, inkl. Erhebung von Steuerungsmaßnahmen
  - 2. Stufe: Plausibilisierung, Bewertung und zentrale Dokumentation der Interessenskonflikte durch das zSM

Reporting

- Der Geschäftsführung ist regelmäßig über die Risiken von wesentlichen Auslagerungen zu berichten (Tz. 102)

Informations-pflichten gegenüber der Aufsicht

- Der Aufsicht ist auf Anforderung das vollständige oder teilweise Auslagerungsregister zur Verfügung zu stellen (Tz. 56)
- Die Informationen sind in einem vereinbarten elektronischen Format bereitzustellen (Tz. 56)
- Auf Anforderung sind alle Informationen zur Verfügung zu stellen, die für eine wirksame Beaufsichtigung erforderlich sind (Tz. 57)
- Rechtzeitige Information über geplante Veränderung bei wesentlichen Auslagerungen (Tz. 58 und Tz. 59)

Pflege des Auslagerungsregisters auf Einzel- und Gruppenebene

NFR-Datenverarbeitung für die OpRisk-Steuerung inkl. Szenarioanalyse

* inkl. Weiterverlagerungen

Risikomanagement und Dienstleistersteuerung im Three-Lines of Defense Modell

Aufgaben der 3rd Line (Internen Revision)

Einbindung im Rahmen ihrer Aufgabe bei der initialen, regelmäßigen und anlassbezogenen Erstellung der Risikoanalyse*

Tätigkeit bezogen auf den Auslagerungs-prozess

- Im Auslagerungsprozess ist durch die Interne Revision mindestens folgendes zu prüfen (Tz. 51):
  - Aufbauorganisation
  - Angemessenheit, Qualität und Wirksamkeit der Bewertung, ob eine Auslagerung eine kritische oder wesentliche Funktion betrifft
  - Angemessenheit, Qualität und Wirksamkeit der Risikobewertung und der Maßnahmen zur Steuerung der Risiken
  - Einbindung des Leitungsorgans in den Auslagerungsprozess
  - Überwachung und Management der Auslagerungsvereinbarungen

Vor-Ort-Kontrollen

- Das Institut übt seine Zugangs- und Prüfungsrechte aus, um u.a. sicherzustellen,
  - dass der Prüfungsplan der Internen Revision des Dienstleisters für die ausgelagerte Funktion angemessen ist (Tz. 93a lit. a)
  - und führt eigene Prüfungshandlungen durch, um z.B. die wichtigsten (Schlüssel-) Kontrollen zu erheben, um sicherzustellen, dass die Prüfungsumfänge der Internen Revision des Dienstleisters in Bezug auf die ausgelagerten Prozesse angemessen sind und für die eigene Dienstleistersteuerung verwendet werden können (Tz. 93 lit. b)

Tätigkeit in Bezug auf die Auslagerung

- Daneben hat die Interne Revision auch den Dienstleister, an den ausgelagert wurde, zu beurteilen (Tz. 50)
- Dafür ist es erforderlich, dass die Interne Revision
  - einen risikobasierten Ansatz für die unabhängige Prüfung von ausgelagerten Tätigkeiten entwickelt und implementiert sowie
  - eine Integration der kritischen und wesentlichen Funktionen in den institutsinternen mehrjährigen Prüfungsplan und in das Prüfungsprogramm vornimmt

* inkl. Weiterverlagerungen

Risikomanagement und Dienstleistersteuerung im Three-Lines of Defense Modell

Beispielhafte Detaildarstellung der Aufgaben der Internen Revision

Umzusetzen seit 2019

Risikoorientierter Ansatz

- Entwicklung eines **risikoorientierten Ansatzes** zur Einbindung der Auslagerungen in den institutsinternen Prüfungsplan
- Der risikoorientierte Ansatz soll dabei die **Wesentlichkeitseinstufung** berücksichtigen; und es ist auch zu berücksichtigen, ob wesentliche Auslagerungen (z.B. auf Grund von Risikokonzentrationen) eine **besondere Tragweite** für das Institut haben
- Über den **risikoorientierten Ansatz** sind alle Auslagerungen zu identifizieren, die im Rahmen der Prüfung zu berücksichtigen sind

Einbindung in die Prüfungsplanung

- Im Prüfungsplan ist der **institutsinterne Auslagerungsprozess** zu berücksichtigen (Tz. 51) sowie die Auslagerungen selbst
- Die Auslagerungen sind auf Basis des entwickelten **risikoorientierten Ansatzes** zu bewerten und zu berücksichtigen
- Bei **Mehrmandantendienstleistern** ist im Rahmen der Prüfungsplanung bereits zu überlegen, ob Joint Audits mit anderen Mandanten durchgeführt werden können und sollen
- **Joint Audits** können durchgeführt werden, wenn
  - alle Institute, die auf den Mehrmandantendienstleister ausgelagert haben, einen gemeinsamen externen Prüfer beauftragen oder
  - jedes Institut einen Prüfer der Internen Revision in das Prüfungsteam des Joint Audits entsendet

Umzusetzen ab 2020

Vor-Ort-Prüfungen

- Auf Basis der Prüfungsplanung sind auch **Vor-Ort-Prüfungen** durchzuführen
- Diese können als **Joint Audits** durchgeführt werden (vgl. „Einbindung in die Prüfungsplanung“)
- Im Rahmen der Vor-Ort Prüfungshandlungen ist u.a. sicherzustellen, dass der **Prüfungsplan der Internen Revision des Dienstleisters** für die ausgelagerte Funktion **angemessen** ist (Tz. 93a lit. a) sowie auch die **Prüfungsdurchführung der Internen Revision** des **Dienstleisters angemessen** ist
- Die Ergebnisse der Prüfung der Kriterien gem. Tz. 93 sind auch an die (ggf. dezentralen) Auslagerungsbeauftragten weiterzugeben, damit diese z.B. die Berichte der Internen Revision des Dienstleisters oder Zertifizierungen durch Dritte als **Informationsquellen für die Überwachung und Steuerung des Dienstleisters** nutzen können

Erfahrungen zur regulatorischen Praxis in Österreich und Deutschland (1/2)

Die Darstellung umfasst Ergebnisse aus Jahresabschlussprüfungen, Sonderprüfungen und Prüfungen der Internen Revision

1 Klassifikation - Prozess
Es besteht kein ganzheitlicher Prozess zur Klassifikation von Fremdbezügen (sFb, sFb IT-DL und Auslagerungen).

2 Klassifikation – Vollständigkeit
Es kann nicht sichergestellt werden, dass alle Fremdbezüge den Klassifikationsprozess durchlaufen.

3 Risikoanalyse – Methode
Im Rahmen der Risikoanalyse zur Einstufung einer Auslagerung werden nicht alle aufsichtsrechtlich definierten K.O.-Kriterien berücksichtigt.

4 Risikoanalyse – Methodik
Im Rahmen der Risikoanalyse werden nicht alle relevanten Abteilungen in die Entscheidung einbezogen (z.B. Compliance, BCM).

5 Risikoanalyse - Methodik
Es findet keine Analyse der Konzentrationsrisiken statt.

6 Risikoanalyse – Operatives Vorgehen
Die in den Risikoanalysen gegebenen Antworten sind nicht nachvollziehbar (nicht ausreichend begründet).

7 Due Diligence - Prozess
Es gibt keinen einheitlichen den aufsichtsrechtlichen Anforderungen entsprechenden Prozess zur Dienstleisterauswahl.

8 Due Diligence – Ergebniswürdigung
Die Ergebnisse der Dienstleisterauswahl werden nicht im Rahmen der Risikoanalyse gewürdigt.

9 Verträge
Insbesondere bei Master-Level-Agreements werden die ausgelagerten Dienstleistungen nicht ausreichend spezifiziert.

10 Service-Level-Agreements
Es werden keine Dienstleistungs- und Dienstleisterspezifischen KPI‘s, KCI oder KRI definiert und auch keine zu erfüllenden Service-Levels sowie Sanktionsmaßnahmen.

Erfahrungen zur regulatorischen Praxis in Österreich und Deutschland (2/2)

Die Darstellung umfasst Ergebnisse aus Jahresabschlussprüfungen, Sonderprüfungen und Prüfungen der Internen Revision

11 NFR – Steuerung

Es findet keine NFR-Steuerung der Auslagerungen und damit kein nachvollziehbarer Einbezug in das Drittparteienrisiko der Bank sowie keine Szenarioanalyse statt.

12 Auslagerungsregister

Die Vollständigkeit des Auslagerungsregisters kann nicht sichergestellt werden.

13 Exit-Strategien

Es bestehen keine Exit-Strategien bzw. die bestehenden Exit-Strategien umfassen für die wesentlichen Auslagerungen keine ausreichenden Desk-Tests der definierten Handlungsoptionen.

14 BCM

Die Auslagerungen werden nicht in die Bankweiten BCM-Konzepte einbezogen.

15 Operative Dienstleistersteuerung

Es findet keine nachvollziehbare Steuerung der Dienstleister statt. Eine nachvollziehbare Validierung der verwendeten Berichte der Dienstleister erfolgt nicht.

16 Interessenkonflikte

Interessenkonflikte (insbesondere bei Gruppeninternen Auslagerungen) werden nicht identifiziert, bewertet und gesteuert. Eine Übersicht über bestehende Interessenkonflikte besteht nicht.

17 Konzentrationsrisiken

Die Risiken daraus, dass

- mehrere Prozesse an einen Dienstleister ausgelagert sind oder
- im Rahmen eines Prozesses mehrere Aktivitäten an unterschiedliche Dienstleister ausgelagert sind,

werden nicht identifiziert, bewertet und gesteuert.

Eine Übersicht über die bestehenden Konzentrationsrisiken besteht nicht.
Ein Einbezug in das NFR erfolgt ebenfalls nicht.

18 Zentrales Sourcing Management

Im Zusammenhang mit dem zentralen Sourcing Management ergaben sich folgende Feststellungen:

- Es besteht kein Kontroll- und Überwachungsplan
- Definierte Kontroll- und Überwachungshandlungen wurden nicht oder nicht nachvollziehbar durchgeführt
- Die Ergebnisse aus Kontroll- und Überwachungshandlungen wurden nicht angemessen verwertet (z.B. kein Einbezug in die Risiko-Assessments)

Deloitte – Risk Advisory | TechCompliance

Bleiben wir in Kontakt

Thomas John
Senior Manager | Risk Advisory

Tel: +43 1 537 00 3723
Mobil: +43 664 80 537 3723
tjohn@deloitte.at

Deloitte Audit Wirtschaftsprüfungs GmbH
Renngasse 1/Freyung
1010 Wien
www.deloitte.at

Bei Fragen oder Anliegen zu den präsentierten Sachverhalten oder damit in Verbindung stehenden Themenbereichen kontaktieren Sie gerne auch unser TechCompliance Team unter

AT TechCompliance

(attechcompliance@deloitte.com)

Deloitte.