BaFin

Bundesanstalt für
Finanzdienstleistungsaufsicht

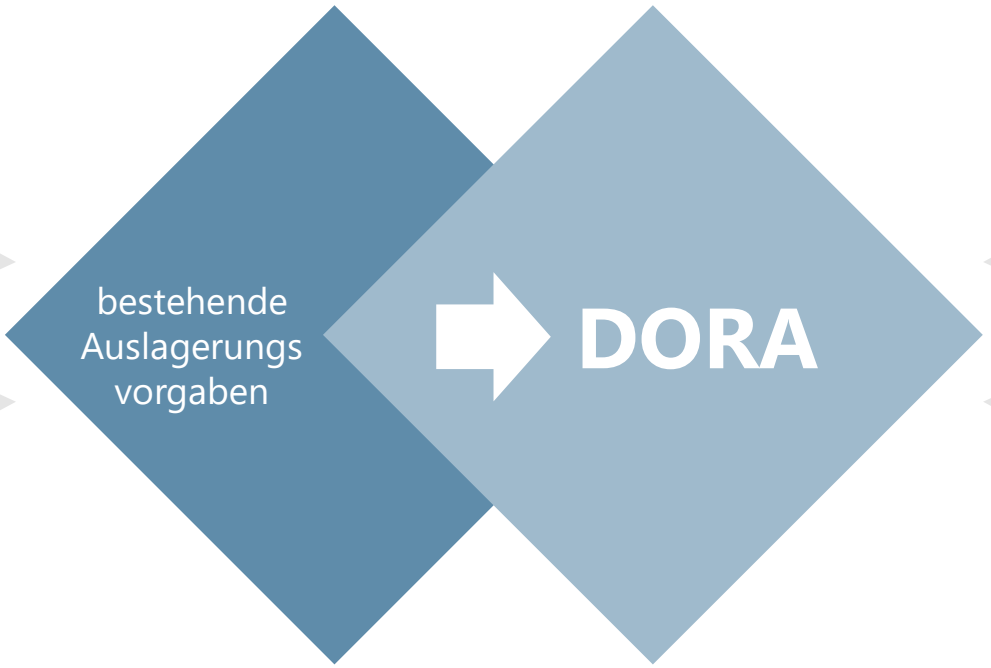
IKT-Drittparteirisikomanagement

Dr. Sven Kleinknecht-Dennart, GIT 3
E-Mail: sven.kleinknecht-dennart@bafin.de

Management des IKT-Drittparteienrisikos

- Vorschriften zu Auslagerungen und ihrer Überwachung sowie Dienstleister-Verträgen sind nicht vollständig in den europäischen Rechtsvor-schriften verankert
- Externe Quellen für IKT-Risiken bei IKT-Dienstleistern werden aktuell nicht ausreichend behandelt

- Mangel an Homogenität und Konvergenz in Bezug auf die Überwachung des IKT-Drittparteienrisikos und die Abhängigkeit von IKT-Drittdienstleistern



- Sektorübergreifend harmonisierte Anforderungen an das IKT-Drittparteirisikomanagement
- Überwachung von kritischen IKT-Drittdienstleistern → identifizierte Risiken dieser IKT-Drittdienstleister sind von den Finanzunternehmen zu berücksichtigen

- Schlüsselprinzipien für das Management des IKT-Drittparteienrisikos
- Festlegung grundlegender vertraglicher Rechte und Pflichten
- Sicherstellung der Fähigkeit, alle von Drittdienstleistern ausgehenden IKT-Risiken wirksam zu überwachen
- Prinzipien ergänzen, die für die Auslagerung geltenden sektorspezifischen Rechtsvorschriften

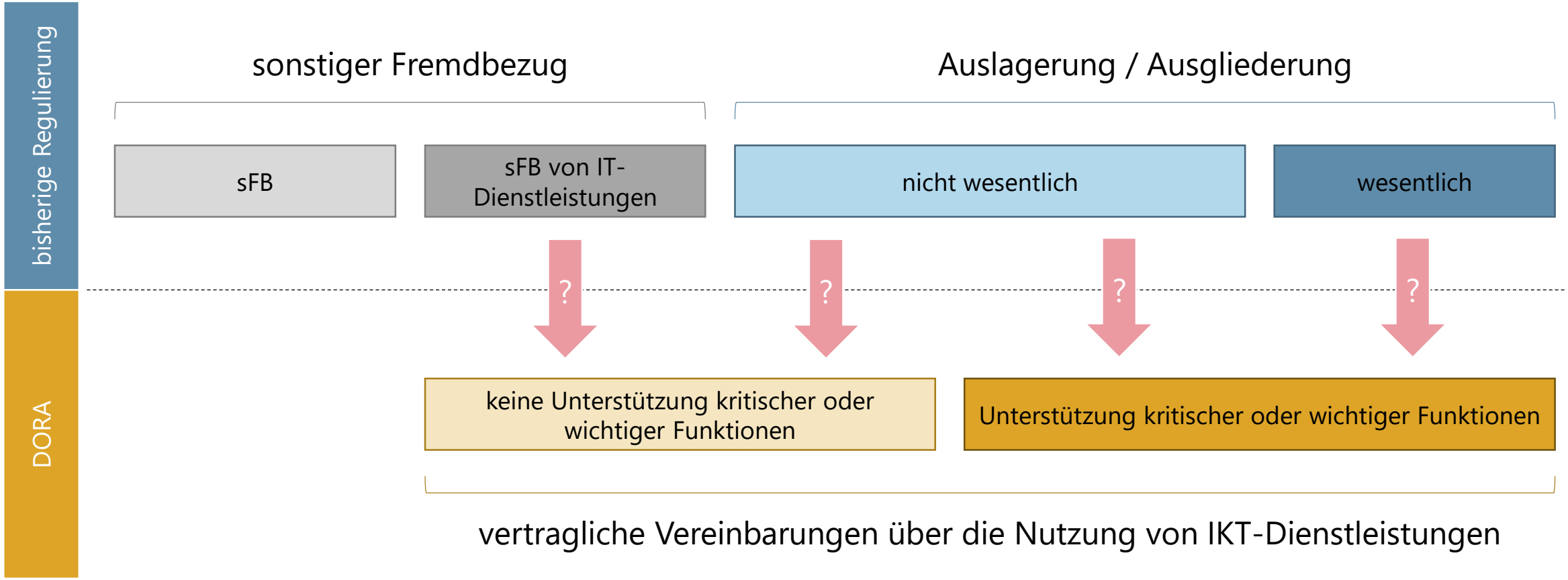
Was sind Vertragsvereinbarungen und IKT-Dienstleistungen?

- Die Definition der vertraglichen Vereinbarungen im Sinne des IKT-Drittparteienrisikos ergibt sich aus Art. 28 (1)(a) und den Begriffsbestimmungen in Art. 3: „*vertragliche Vereinbarungen des Finanzunternehmens über die dauerhafte Nutzung von IKT-Dienstleistungen mit IKT-Drittdienstleistern für die Ausübung ihrer Geschäftstätigkeit*".
- Auflistung von beispielhaften IKT-Dienstleistungen können indikativ herangezogen werden, um Erwartungen in Bezug auf häufig anfallende Arten von IKT-Dienstleistungen abzuschätzen. Die Liste findet sich im Anhang IV des Konsultationsentwurfs zum ITS-Informationsregister *("Implementing technical standards with regard to standard templates for the register of information")*.

Miete von Soft- und Hardware	**Datendienste**	**Betriebsunterstützung**	**andere Unterstützung**	**Andere**
Miete Software Lizenzen	Datenbezug	IKT-Help Desk / -Incident	IKT-Projektmanagement	Telekommunikations-dienstleister
IKT-Räumlichkeiten (z. B. RZ)	Datenanalysen	IKT-Sicherheit	IKT-Entwicklung	Cloud (IaaS)
Rechenkapazität (auch Cloud)		IKT-Betrieb (ohne Netz)	IKT-Beratung	Cloud (PaaS)
Speicherkapazität (keine Cloud)		Netzwerk Dienstleistungen	IKT-Risikomanagement und -Prüfung	Cloud (SaaS)
Miete Netzwerkgeräte				alle weiteren IKT Dienstleistungen
Miete Hardware				

Neue Kategorien im IKT- Drittparteirisikomanagement

Unterscheidung zwischen IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen, und solchen, die dies nicht tun. Kritisch oder wichtig sind Funktionen, wenn ihr Ausfall eine erhebliche Beeinträchtigung der finanziellen Leistungsfähigkeit, der Geschäftsfortführung oder regulatorischer Art darstellen würde. (Art. 3(22))



Prinzipien für das Management von IKT-Drittparteienrisiken

Verantwortung	Finanzunternehmen bleiben jederzeit im vollen Umfang für die Einhaltung und Erfüllung aller Verpflichtungen (DORA & Finanzdienstleistungs-recht) verantwortlich.
Grundsatz der Verhältnismäßigkeit	Das Management des IKT-Drittparteienrisikos orientiert sich an den IKT-bezogenen Abhängigkeiten, den Risiken aus der Drittvergabe, der Kritikalität der betroffenen Funktion und den Auswirkungen auf Kontinuität und Verfügbarkeit.
Strategien	Strategie für das IKT-Drittparteienrisiko (ggf. unter Beachtung der Mehranbieter-Strategie) und eine dazugehörige Leitlinie zur Nutzung von Dienstleistungen von IKT-Drittdienstleistern zur Unterstützung kritischer oder wichtiger Funktionen
Überprüfung Risiken	Leitungsorgan prüft regelmäßig auf Grundlage des Gesamtrisikoprofils Risiken aus der Nutzung von IKT-Drittdienstleistern, bezogen auf kritische oder wichtige Funktionen.
Interne Berichtspflichten	Leitungsorgan ist zu informieren über: Vertragsvereinbarungen, relevante geplante wesentlichen Änderungen in Bezug auf IKT-Drittdienstleister, inkl. potenzieller Auswirkungen auf kritische oder wichtige Funktionen.
Informations-register	Führung eines Informationsregisters mit allen vertraglichen Vereinbarungen; jährliche Meldung eines Berichts an die Aufsicht; auf Verlangen Vorlage des Informationsregisters
Meldepflicht	Zeitnahe Unterrichtung der zuständigen Behörde über jede geplante vertragliche Vereinbarung zur Unterstützung kritischer oder wichtiger Funktionen.
Überwachungs-funktion	Einrichtung einer Überwachungsfunktion zur Nutzung von IKT-Drittdienstleistern (oder Übernahme durch ein Mitglied der Geschäftsleitung).

Lebenszyklus der vertraglichen Vereinbarung

- **Ausstieg und Beendigung** der vertraglichen Vereinbarung (Art. 11)
  Pläne sollen realistisch und durchführbar sein, auf plausiblen Szenarien und sinnvollen/angemessenen Annahmen beruhen

- **Governance-Prinzipien** (Art. 3)
- Proportionalität (Art. 1)
- Anwendungsbereich (Art. 2)
- Arten von IKT-Drittparteidienstleistern (Art. 4)
- Dokumentation und Aufbewahrungspflichten (Art. 5)

- **Überwachung** (Art. 10)
  Laufende Überwachung der Leistungsfähigkeit des Dienstleisters über Indikatoren, auch der Sicherheit und der Einhaltung interner Vorgaben; Auswertung der Berichterstattung (Vorfälle, Betrieb, Sicherheit, BCM);
  Auswertung von Prüfungen, Reviews, KCIs;
  Durchführung von eigenen Prüfungen;
  Maßnahmen müssen definiert und dokumentiert nachgehalten werden

- **Ex-ante Risikoanalysen** (Art. 6)
  dabei Definition des „business needs" bezogen auf die IKT-Dienstleistung und Berücksich-tigung aller relevanten Risiken aus DORA und sektorspezifischen Regelungen sowie Mindest-risikokatalog
- **Due Diligence** (Art. 7)
  darunter: Fähigkeiten des IKT-Dienstleisters, Nutzung Unterauftragnehmer, Drittstaaten-bezug, Audits, ESG, Nachweisbarkeit „level of assurance"
- **Interessenskonflikte** (Art. 8)

- **Vertragsinhalte** (Art. 9 und Art. 3)
  Mindestvertragsinhalte aus Level 1, Art der Nutzung von Prüfungsrechten, Voraussetzungen bei Nutzung von Zertifikaten und Prüfberichten Dritter und Auswirkungen auf den Vertrag, Vorgaben zur Form bei Änderungen

- Einbindung der Geschäftsleitung (Art. 5)
- Einbindung des Geschäftsbereichs (Art. 5)
- Einbindung von Kontrollfunktionen (Art. 5)

Wann sind IKT-Dienstleister geeignet?

nicht kritisch/wichtig

- Einhaltung angemessener Standards für Informationssicherheit
- Verpflichtung zur Zusammenarbeit mit zuständigen Aufsichtsbehörden
- Teilnahme an den Sensibilisierungs-programmen und Schulungen zur IKT-Sicherheit/DOR

kritisch/wichtig (zusätzlich)

- Anwendung aktuellster und höchster Qualitätsstandards für die Informationssicherheit
- Meldung aller Entwicklungen mit wesentlichen Einfluss auf kritische/wichtige Funktionen
- Implementierung und Test von Notfallplänen
- Verfügt über Maßnahmen, Tools und Leit- und Richtlinien zur IKT-Sicherheit
- Beteiligung an TLPT

Grundsätzliche Bedingungen

Die Betrachtung der Risiken kommt im Rahmen der Risikoanalyse und der Due Diligence hinzu

Landkarte IKT-Drittparteirisiken

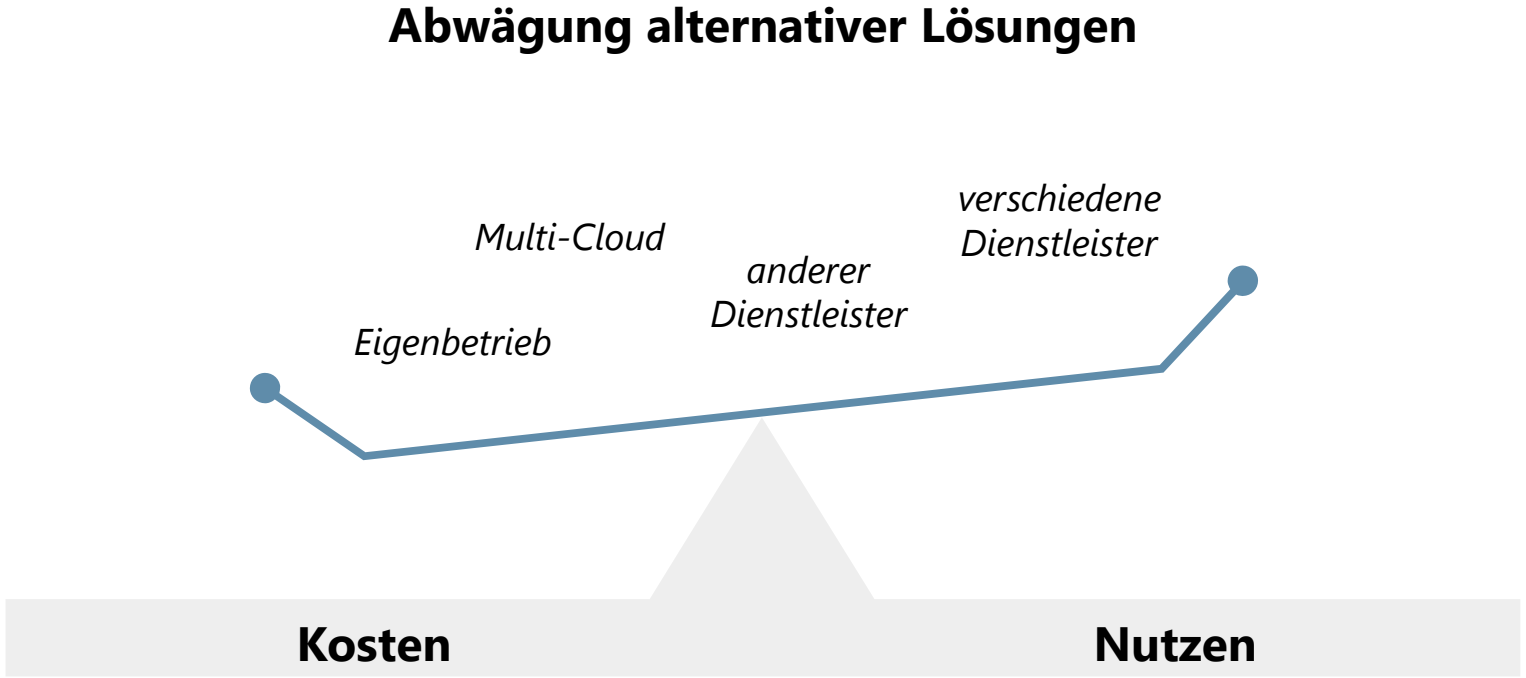
- Es sind **alle relevanten Risiken** im Zusammenhang mit einer vertraglichen Vereinbarung zu **ermitteln** und zu **bewerten**
- Die Risikobewertung muss **vor dem Abschluss** der vertraglichen Vereinbarung vorgenommen werden
- Besonderes Augenmerk ist auf das **IKT-Konzentrationsrisiko** zu legen
- Der RTS detailliert für kritische/ wichtige Vertragsvereinbarungen Mindestrisikokategorien in Art. 6 (2)

*Level 2

Bewertung von Konzentrationsrisiken

Verträge mit einem IKT-Drittdienstleister, der nicht ohne Weiteres ersetzbar ist

mehrfache vertragliche Vereinbarungen mit demselben IKT-Dienstleister



- Wahrscheinlichkeit des Auftretens ist zu ermitteln, auch durch Analysen von Unterauftragsvereinbarungen
- Zielkonflikt zwischen Finanzstabilität und Vertragsfreiheit:
  - Abwägung von Kosten und Nutzen, unter Berücksichtigung der geschäftlichen Erfordernisse und der Strategie für digitale operationelle Resilienz
  - Ansatz um flexibel und schrittweise" Konzentrationsrisiken zu reduzieren

Wesentliche Vertragsbestimmungen

Eindeutige Zuweisung von Rechten und Pflichten in einem schriftlichen Dokument

Erwägung von Standardvertrags-klauseln

Elemente für **alle** vertraglichen Vereinbarungen

- Klare, vollständige Beschreibung
- Standort der Daten
- Datenschutz
- Zugang zu Daten bei Insolvenz
- Dienstleistungsgüte
- Unterstützung bei Vorfällen
- Kooperation mit Aufsichtsbehörden
- Kündigungsfristen
- Schulungen

Elemente bei **kritischen oder wichtigen** Funktionen

- KPIs für Leistungsziele
- Berichtspflichten des Dienstleisters
- Notfallpläne
- Beteiligung an TLPT
- Prüfrechte
- Ausstiegsstrategien

Ausstiegsstrategien und -pläne

Risiken, die einen Ausstieg auslösen können:

- **Fehler** des IKT-Drittdienstleisters oder eine **Verschlechterung der Qualität**
- Jede **Unterbrechung der Geschäftstätigkeit** aufgrund unangemessener oder unterlassener Bereitstellung von IKT-Dienstleistungen
- Jedes **erhebliche Risiko** im Zusammenhang mit der angemessenen und kontinuierlichen Bereitstellung von IKT-Dienstleistungen
- **Beendigung der Vertragsvereinbarung** aufgrund:
  - erheblichem Verstoß gegen Gesetze, Vorschriften oder Vertragsbedingungen
  - Umstände und Änderungen, die zu Beeinträchtigungen führen werden
  - nachweislichen Schwächen im IKT-Risikomanagement
  - Beeinträchtigung der Beaufsichtigung

Ziel: effektiv zu anderen IKT-Drittdienstleistern wechseln oder alternativ zu internen Lösungen wechseln

Maßnahmen:

- Ausstiegsstrategien auf Basis der Risiken
- Alternative Lösungen und Übergangspläne um sichere und vollständige Migration zu gewährleisten
- Ausstiegspläne müssen umfassend, dokumentiert und getestet sein
- Regelmäßige Überprüfung

BaFin

Bundesanstalt für
Finanzdienstleistungsaufsicht

Vielen Dank für Ihre Aufmerksamkeit!