BaFin

Bundesanstalt für
Finanzdienstleistungsaufsicht

DORA für IKT-Drittdienstleister

Gruppe IT-Aufsicht und Cybersicherheit

BaFin
Bundesanstalt für
Finanzdienstleistungsaufsicht

Begrüßung

Jens Obermöller,
Leiter der Gruppe IT-Aufsicht und Cybersicherheit

BaFin

Bundesanstalt für
Finanzdienstleistungsaufsicht

Update DORA und deutscher Ansatz zur Überwachung von IKT-Drittdienstleistern

Janusz Dreier

Abhängigkeit des Finanzmarkts von Drittdienstleistern

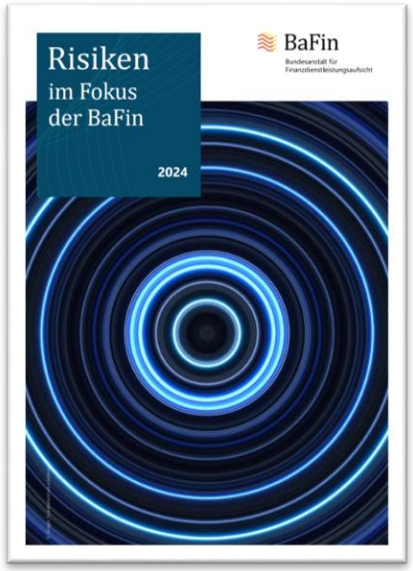


Abb. 1: In dem Bericht „Risiken im Fokus der BaFin 2024" stellt die BaFin die Risiken zusammen, welche die Finanzstabilität oder die Integrität der Finanzmärkte in Deutschland am meisten gefährden können. Dazu gehören auch Risiken aus Konzentrationen bei der Auslagerung von IT-Dienstleistungen, Link

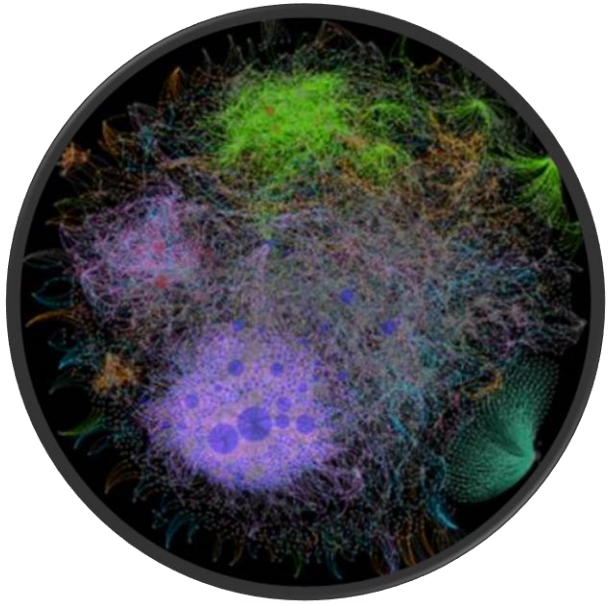


Abb. 2: Der Netzwerkgraph visualisiert die Verflechtungen von Auslagerungen auf dem gesamten deutschen Finanzmarkt auf Grundlage der Auslagerungsdatenbank der BaFin.

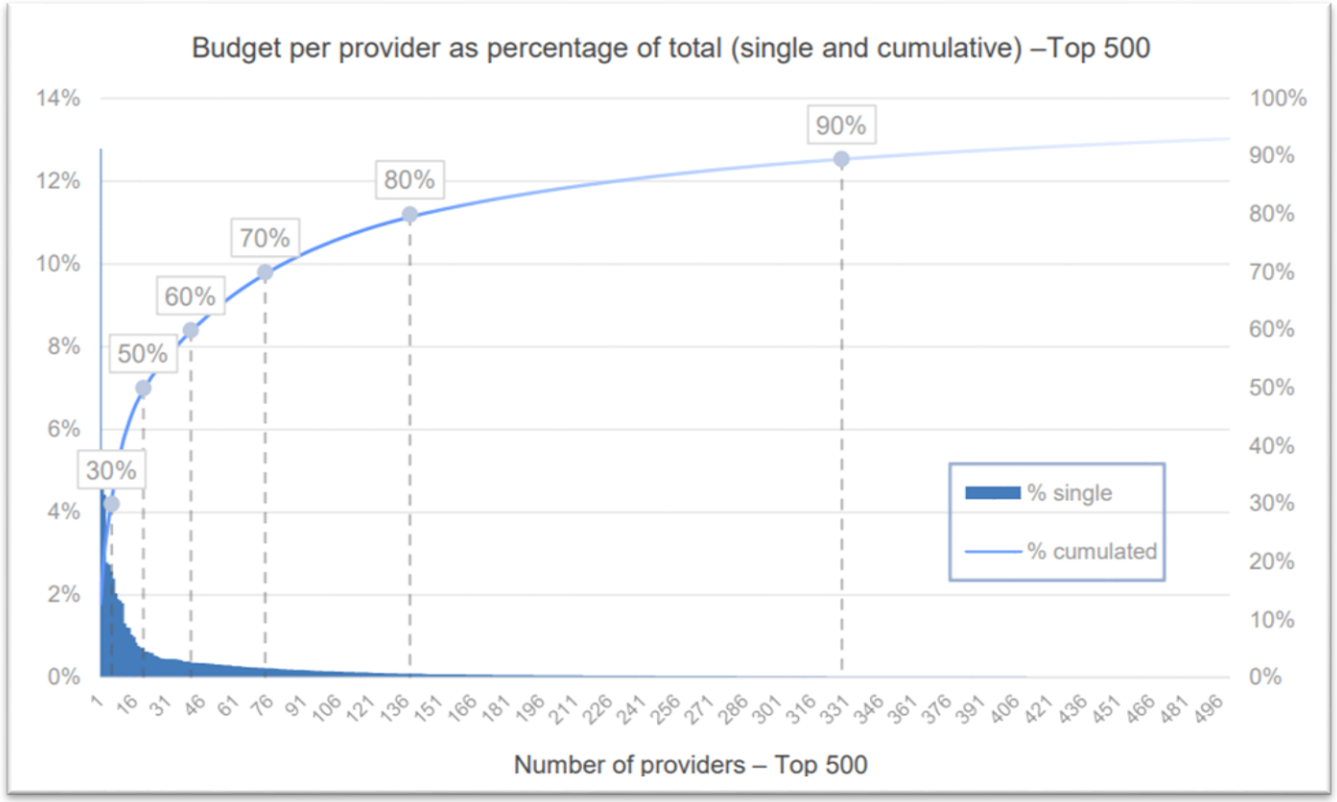


Abb. 3: European Central Bank, Outsourcing register – Annual horizontal analysis, 21 February 2024, S. 9, Link

Überwachung von IKT-Drittdienstleistern: Historie

Bis 2022

- Keine sektorweit einheitlichen aufsichtlichen Befugnisse unmittelbar gegenüber Dienstleistern

Das Gesetz zur Stärkung der Finanzmarktintegrität (FISG) ist am 01. Januar 2022 vollständig in Kraft getreten

Inkrafttreten des Digital Operational Resilience Act (DORA) am 17. Januar 2023

Anwendung von DORA ab dem 17. Januar 2025

Seit 2022

Sektorweit einheitliche

- Anzeigepflicht für Auslagerungen
- unmittelbare Informations- und Prüfungsrechte gegenüber Auslagerungsunternehmen
- unmittelbare Befugnis zur Anordnung von Maßnahmen zur Missstandsvermeidung und Missstandsbeseitigung, inkl. Bußgeld

Ab 2025

- DORA ermöglicht die Überwachung von kritischen IKT-Drittdienstleistern auf europäischer Ebene

DORA: Digital Operational Resilience Act

Hintergrund

- DORA ist Teil des **Digital Finance Package der EU KOM** von 2020 bestehend aus:
  - DORA Regulation
  - MiCA Regulation (Markets in Crypto Assets)
  - Retail Payment Strategy
  - digitale Finanzstrategie
- Aufbauend auf dem FinTech Action Plan (2018) und dem Joint Advice der ESAs (2019)

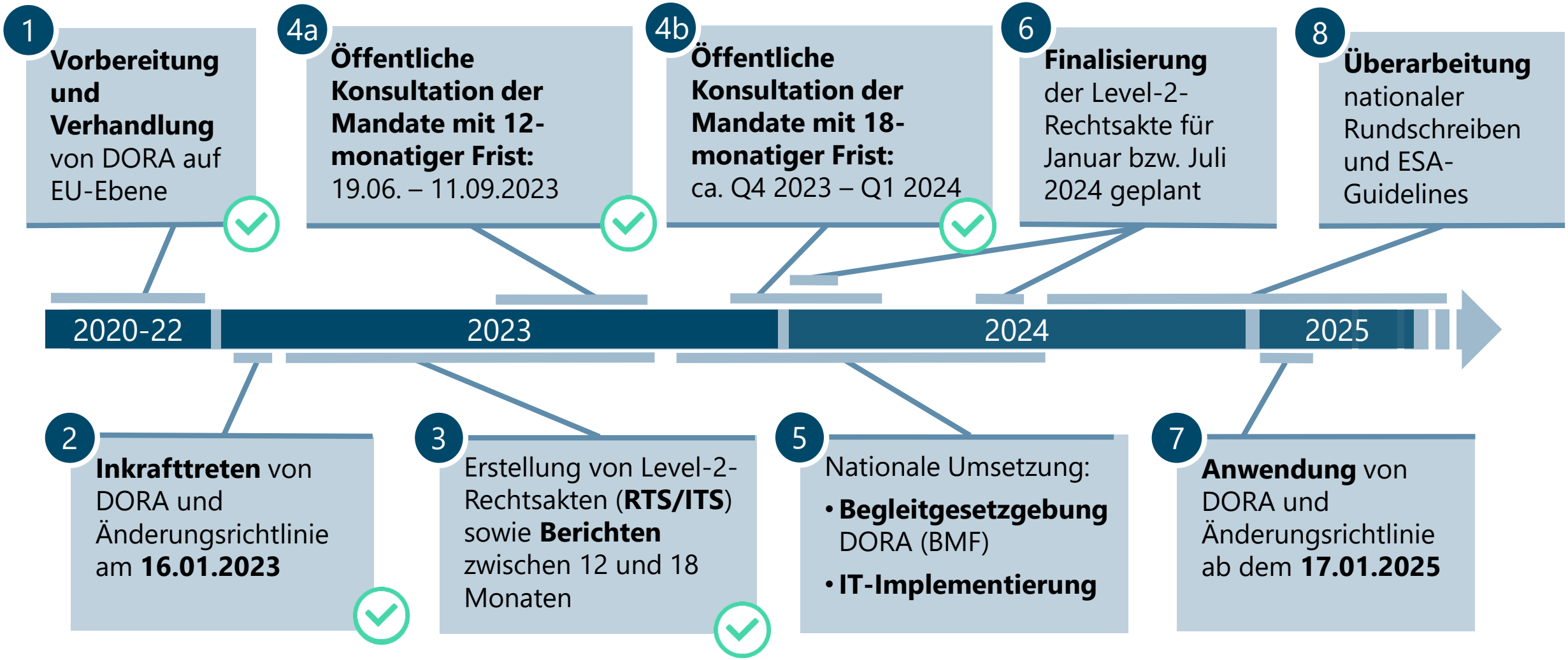
Ziele

- Stärkung der **Sicherheit und operationalen Resilienz** des gesamten europäischen Finanzsektors
- Schaffung **einheitlicher und konsistenter Anforderungen** für den gesamten Finanzsektor
- Einführung proportionaler Anforderungen **(Prinzip der Proportionalität)**

Anwendungsbereich

- **Finanzsektorübergreifend**
- CRR-Kreditinstitute, Zahlungsinstitute (einschließlich registrierter Kontoinformationsdienstleister), E-Geld-Institute, Wertpapierfirmen, Anbieter von Krypto-Dienstleistungen (MiCA), CSD, CCP, Handelsplätze, Transaktionsregister, Verwaltungsgesellschaften, AIFM, Datenbereitstellungsdienste, Versicherungs- und Rückversicherungsunternehmen, Versicherungsvermittler, EbAVs, Ratingagenturen, Administratoren kritischer Referenzwerte, Verbriefungsregister, Schwarmfinanzierungsdienstleister

Vergangenes, Aktuelles und nächste Schritte



Wesentliche Elemente in DORA

IKT-Risikomanagement

- **Governance und Organisation**
- **IKT-Risikomanagement-rahmen**
- **IKT -Systeme, -Protokolle und –Tools**
- **Lernprozesse und Weiterentwicklung**
- **Kommunikation**

IKT-Drittparteirisikomanagement

- **Allgemeine Prinzipien** (u. a. Informationsregister über IKT-Drittparteivertragsbeziehungen, Mitteilungen an die Aufsichtsbehörden, und Mindestvertragsbestandteile)

EU-Überwachungsrahmenwerk

- Überwachung von **kritischen IKT-Drittdienstleistern**

IKT-Vorfallmeldewesen

- Festlegung von **Definitionen** IKT-bezogener Vorfälle
- **Klassifikationskriterien** von IKT-bezogenen Vorfällen
- **Meldeprozess,** Berichtswesen von IKT-bezogenen Vorfällen und Cyberbedrohungen

Testen der digitalen operationalen Resilienz

- **Basistests**
- Gesamter Finanzsektor
- Schwachstellenscans, Quellcodetests, Performancetests etc.

TLPT

- **Fortgeschrittene Tests**
- TLPT: Threat Led Penetration Tests
- Nur „systemrelevante“ Finanzunternehmen mit hohem IKT-Reifegrad
- TIBER-EU als „Blaupause“

Information Sharing & Cyberübungen

- Freiwilliger **Austausch von Informationen und Erkenntnissen** zwischen Finanzunternehmen zur Verbesserung der „Situational Awareness“
- Sektorübergreifende **Krisenmanagement- und Notfallübungen** mit Cyberbezug zur Verbesserung der Kommunikation und Stärkung der Resilienz im Finanzsektor

IKT-Drittdienstleister und IKT-Dienstleistungen i.S.v. DORA

- **IKT-Drittdienstleister** ist ein „*Unternehmen, das IKT-Dienstleistungen anbietet*" (Art. 3 Nr. 19 DORA).

- **IKT-Dienstleistungen**:
  - Gem. Art 3 Nr. 21 DORA handelt es sich dabei um „*digitale Dienste und Datendienste, die über IKT-Systeme einem oder mehreren internen oder externen Nutzern dauerhaft bereitgestellt werden, einschließlich Hardware als Dienstleistung und Hardwaredienstleistungen, wozu auch technische Unterstützung durch den Hardwareanbieter mittels Software- oder Firmware-Aktualisierungen gehört, mit Ausnahme herkömmlicher analoger Telefondienste*"
  - Auflistung von beispielhaften IKT-Dienstleistungen in Anhang III des Entwurfs der europäischen Aufsichtsbehörden zum ITS-Informationsregister *("Implementing technical standards with regard to standard templates for the register of information")* kann indikativ herangezogen werden, um Erwartungen in Bezug auf häufig anfallende Arten von IKT-Dienstleistungen abzuschätzen.

Soft- und Hardware	Datendienste	Betrieb	Cloud	Betriebsunterstützung	andere Unterstützung	Andere
Software Lizenzen (ohne SaaS)	Datenbezug	IKT-Räumlichkeiten und Hosting (keine Cloud)	IaaS	IKT-Help Desk / -Incident	IKT-Projektmanagement	Telekommunikations-dienstleister
Hardware als Dienstleistung	Datenanalysen	Rechenkapazität (auch Cloud)	PaaS	IKT-Sicherheit	IKT-Entwicklung	
		Speicherkapazität (keine Cloud)	SaaS	IKT-Betrieb (ohne Netz)	IKT-Beratung	
				Netzwerk Infrastruktur	IKT-Risikomanagement	

BaFin

Bundesanstalt für
Finanzdienstleistungsaufsicht

Virtuelle Fragerunde zur Überwachung von IKT-Drittdienstleistern

Janusz Dreier

BaFin

Bundesanstalt für
Finanzdienstleistungsaufsicht

Europäischer Überwachungsrahmen für kritische IKT-Drittdienstleister

Dr. Sibel Kocatepe

Europäische Überwachung kritischer IKT-Drittdienstleister

- Neues Element der EU-Finanzregulierung stellt **keine direkte Aufsicht** über kritische IKT-Drittdienstleister dar (vgl. Erwägungsgrund 76 DORA).
- Die Aufsicht überwacht kritische IKT-Drittdienstleister mit Blick auf den gesamten Finanzmarkt.
- Der **Überwachungsumfang** der Aufsicht beschränkt sich auf (vgl. Art. 33 Abs. 3 DORA):

IKT-Anforderungen zur Gewährleistung der Sicherheit, Verfügbarkeit, Kontinuität, Skalierbarkeit und Qualität der Dienste

Physische Sicherheit

Risikomanagement-prozesse

Governance-Regelungen zur Sicherstellung eines wirksamen IKT-Risikomanagements

Ermittlung, Überwachung und unverzügliche Meldung IKT-bezogener Vorfälle

Mechanismen für Datenübertragbarkeit, Übertragbarkeit von Anwendungen und Interoperabilität

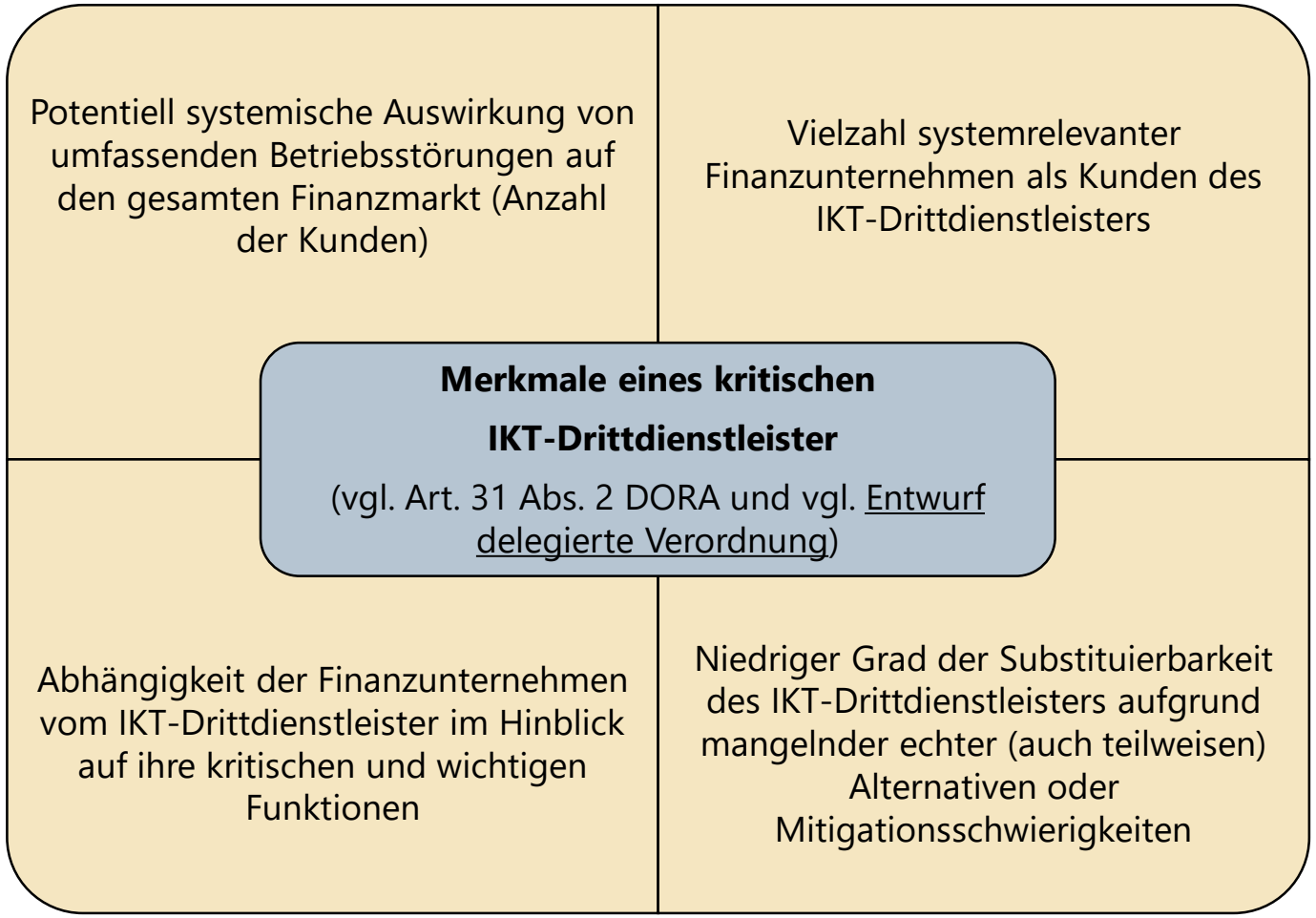
Tests von IKT-Systemen, Infrastrukturen und Kontrollen

IKT-Audits

Übernahme einschlägiger nationaler und internationaler Normen

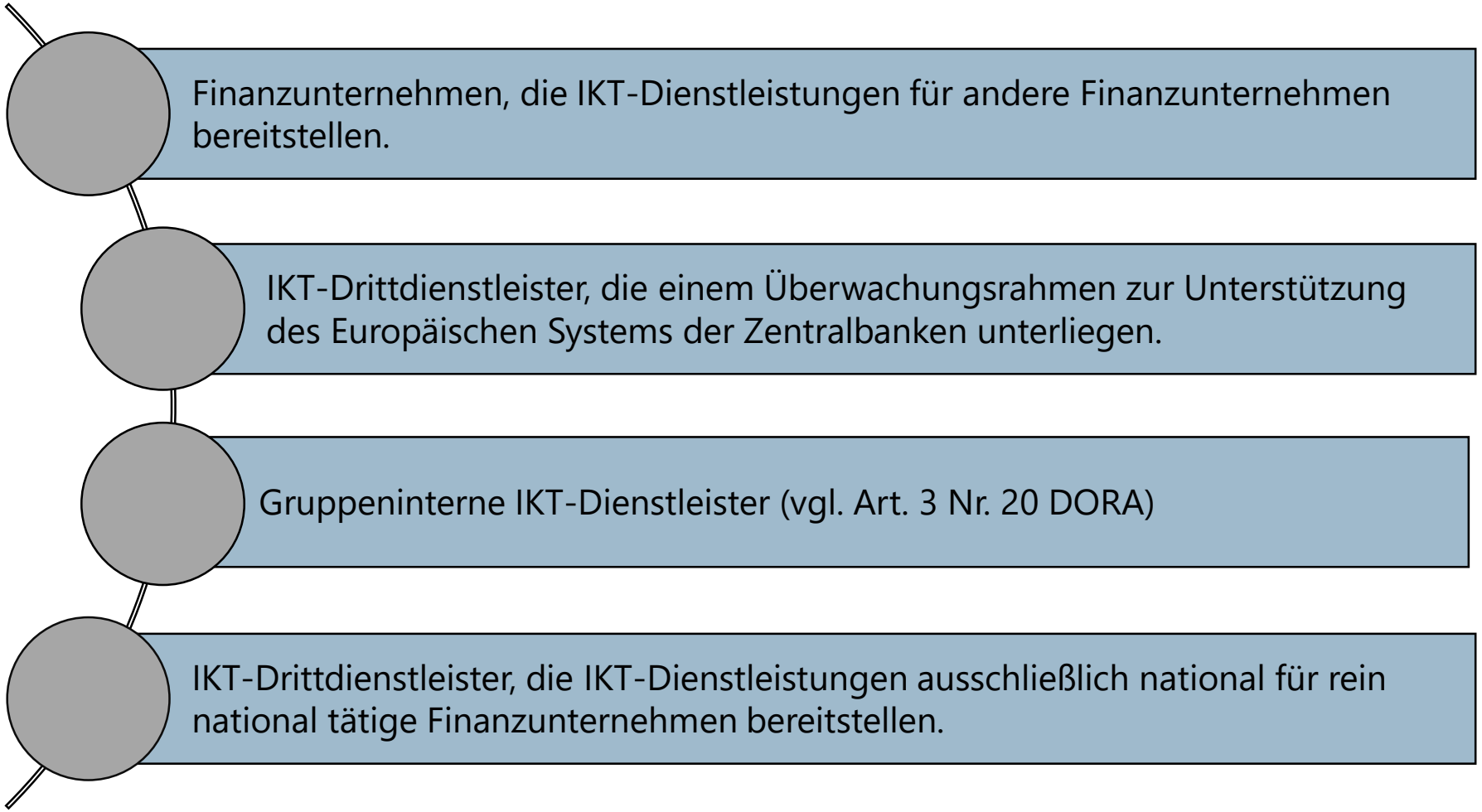
Kritischer IKT-Drittdienstleister

- **Kritischer IKT-Drittdienstleister** ist ein *„IKT-Drittdienstleister, der gemäß Art. 31 DORA als kritisch eingestuft wurde“* (Art. 3 Nr. 23 DORA).
- **Anbieter von Cloud-Computing-Diensten** stehen im Fokus des europäischen Gesetzgebers bei der Entwicklung des Überwachungsrahmenwerks (vgl. Erwägungsgrund 20 DORA).



Kritischer IKT-Drittdienstleister: Ausnahmen

Gemäß Art. 31 Abs. 8 DORA sind bestimmte IKT-Drittdienstleister von der Überwachung durch die europäischen Aufsichtsbehörden ausgeschlossen.



Die Einstufung als kritischer IKT-Drittdienstleister

Ermittlung kritischer IKT-Drittdienstleister: Prüfung erfolgt durch die europäischen Aufsichtsbehörden im Einzelfall u.a. auf Grundlage der vollständigen Informationsregister der Finanzunternehmen und der Kritikalitätskriterien der delegierten Verordnung (vgl. Konsultationsfassung).

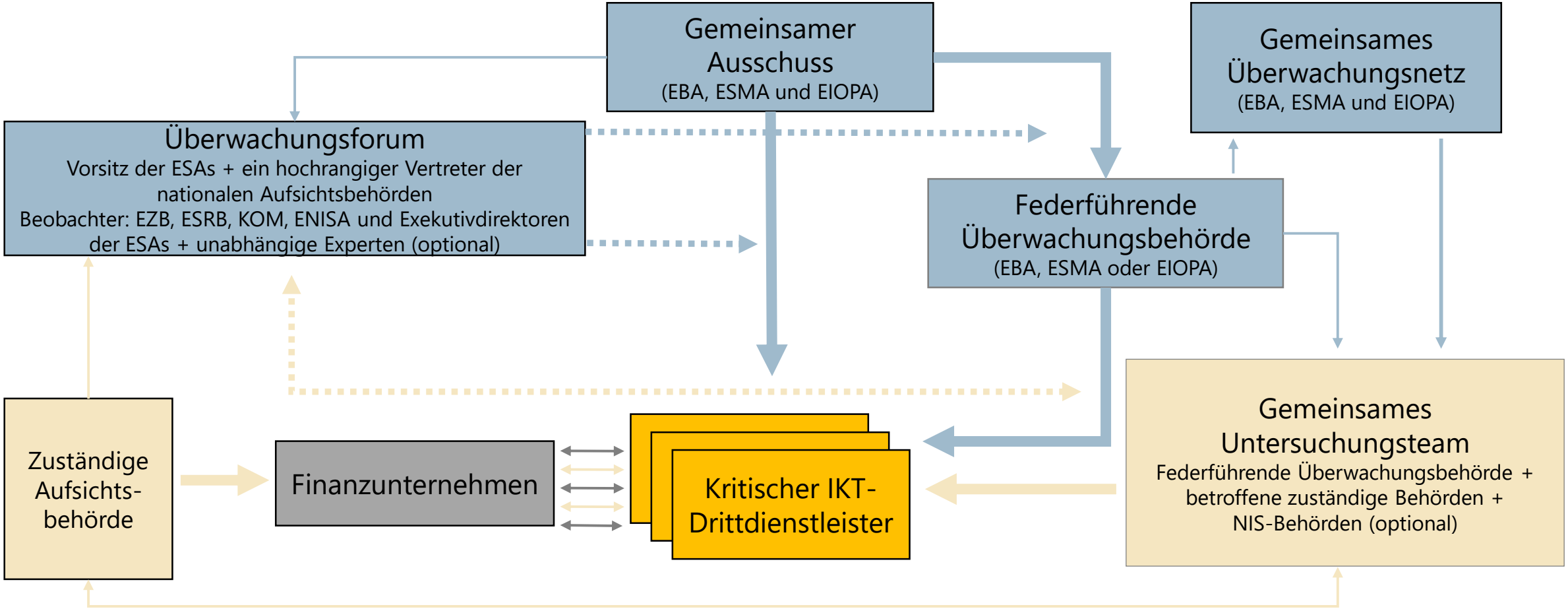
Anhörung: IKT-Drittdienstleister erhält von den europäischen Aufsichtsbehörden die Möglichkeit zur Stellungnahme zur geplanten Einstufung als kritischer IKT-Drittdienstleister mit einer Frist von 6 Wochen.

Einstufungsanordnung: Kritischer IKT-Drittdienstleister erhält Mitteilung über seine Einstufung und den Beginn der Überwachungstätigkeiten (max. 1 Monat nach Mitteilung).

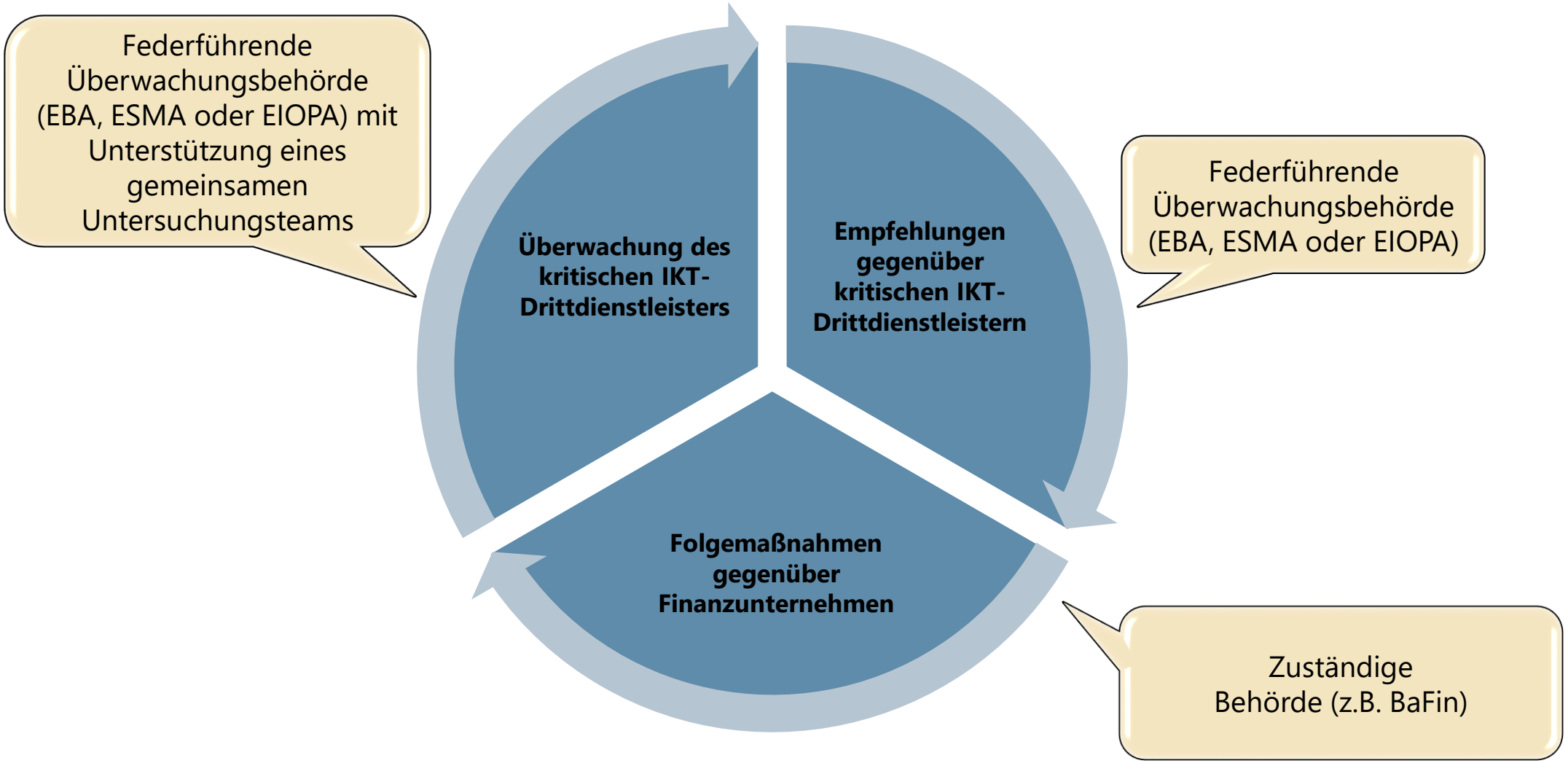
Sitz in der EU: Kritische IKT-Drittdienstleister mit Sitz in einem Drittland müssen binnen zwölf Monaten nach ihrer Einstufung ein Tochterunternehmen in der EU gründen.

Kostentragung: Die Kosten der Überwachung tragen die kritischen IKT-Drittdienstleister entsprechend der delegierten Verordnung (vgl. Konsultationsfassung).

Überwachungsrahmenwerk



Zuständigkeiten im Überwachungszyklus



Der Überwachungszyklus

Überwachungstätigkeiten

- Die europäischen Aufsichtsbehörden erstellen **jährlich** einen **individuellen risikobasierten Überwachungsplan (inkl. Überwachungszielen und Überwachungsmaßnahmen)** für den kritischen IKT-Drittdienstleister.
- Die europäischen Aufsichtsbehörden haben gegenüber kritischen IKT-Drittdienstleistern die folgenden **Überwachungsbefugnisse**:
  - Anforderung von Informationen und Unterlagen
  - Durchführung von Prüfungen
  - Anforderung von Berichten zu Maßnahmen in Folge der Empfehlungen
- **Durchsetzung der Befugnisse:**
  - Verhängung von Zwangsgeldern mit Veröffentlichung
  - Täglich bis zu **1% des durchschnittlichen weltweiten Tagesumsatzes** des vergangenen Geschäftsjahres, max. 180 Tage

Empfehlungen

- Die europäischen Aufsichtsbehörden können **Empfehlungen** gegenüber dem kritischen IKT-Drittdienstleister abgeben, insb. im Hinblick auf die Anwendung von IKT-Sicherheits- und Qualitätsanforderungen oder -verfahren.
  - Kritische IKT-Drittdienstleister müssen binnen **60 Tagen** nach Erhalt der Empfehlung erklären, ob sie den Empfehlungen Folge leisten oder begründen, warum sie dies nicht tun.
  - Nicht erfolgte oder unzureichende Erklärungen werden grds. von den europäischen Aufsichtsbehörden **veröffentlicht**.
- Der kritische IKT-Drittdienstleister erstellt einen **Plan zur Mitigation der aufgezeigten Risiken** und legt auf Verlangen **Fortschrittsberichte** dazu vor.
- Die europäischen Aufsichtsbehörden können nach Abschluss der Überwachungstätigkeiten **Berichte** über die (Abhilfe-)Maßnahmen im Hinblick auf die ausgesprochenen Empfehlungen anfordern.

Folgemaßnahmen

- Die zuständigen Behörden prüfen **risikobasiert** und nach dem **Grundsatz der Proportionalität**, wie die Finanzunternehmen die in den Empfehlungen festgestellten **Risiken** beim kritischen IKT-Drittdienstleister zu berücksichtigen planen.
- Bei **nicht oder nicht ausreichender Berücksichtigung der Risiken** durch Finanzunternehmen, teilt die nationale Behörde ihre Einschätzung dem Finanzunternehmen mit und kann binnen 60 Tagen nach dieser Mitteilung als **letztes Mittel** von Finanzunternehmen verlangen,
  - die Nutzung des kritischen IKT-Drittdienstleisters **ganz oder teilweise zu unterbrechen**, bis die Risiken beseitigt sind, oder
  - die Verträge mit dem kritischen IKT-Drittdienstleister **ganz oder teilweise zu kündigen**.

BaFin

Bundesanstalt für
Finanzdienstleistungsaufsicht

Pause

BaFin

Bundesanstalt für
Finanzdienstleistungsaufsicht

Virtuelle Fragerunde zum Überwachungsrahmen für kritische IKT-Drittdienstleister

Dr. Sibel Kocatepe

BaFin

Bundesanstalt für
Finanzdienstleistungsaufsicht

Vertragliche Anforderungen an die Nutzung von IKT-Dienstleistungen

Dr. Sven Kleinknecht-Dennart

DORA bringt deutliche Ausweitung der Vertragsinhalte

DORA identifiziert Herausforderungen und geht diese an:

- Schwierigkeiten Verträge mit IKT-Drittdienstleistern zu verhandeln, die das Aufsichtsrecht ausreichend umsetzen
- Defizite bei der Durchsetzung von bestimmten Rechten, auch wenn diese eigentlich in den Verträgen verankert sind, insbesondere bei den Prüfrechten und den Unterauftragsvergaben
- Hoch standardisierte Dienstleistungen mit standardisierten Verträgen, die die spezifischen Anforderungen der Finanzbranche nicht abbilden

Ziel:
Formulierung von grundlegenden „Mindestgarantien" in den Verträgen, die die Schlüsselprinzipien eines guten IKT-Drittparteienrisikomanagements unterstützen:

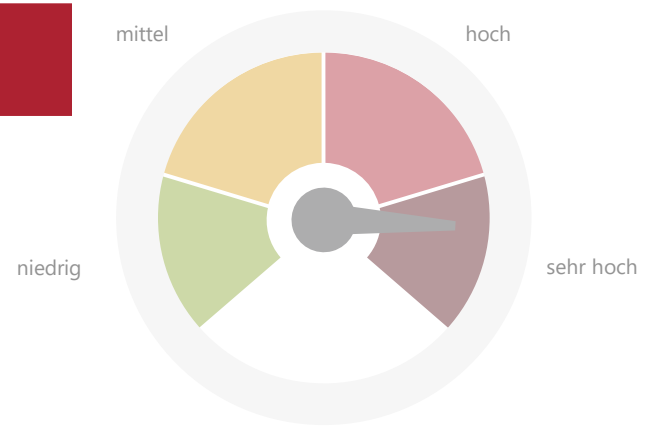
- Erfüllung der Dienstleistung
- Beendigung der vertraglichen Vereinbarung
- wirksame Überwachung des IKT-Drittdienstleisters

Mit DORA geht eine deutliche Ausweitung der verpflichtend mit dem IKT-Dienstleister zu vereinbarenden Vertragsinhalte einher. Dadurch ist in vielen Fällen eine Neu- bzw. Nachverhandlung von Verträgen mit IKT-Drittdienstleistern notwendig. Hinzu kommt, dass die verpflichtenden Vertragsinhalte auch vertragliche Vereinbarungen abdecken, die nicht kritische oder wichtige Funktionen unterstützen, bzw. keine wesentlichen Auslagerungen betreffen.

Hinweis:
DORA ergänzt die geltenden sektorspezifischen Rechtsvorschriften (siehe Erwägungsgrund 29)

Top 5 Änderungen im IKT-Drittparteirisikomanagement

1. Durch die deutliche Ausweitung des Anwendungsbereichs und der verpflichtend zu vereinbarenden Vertragsinhalte ist eine Neu- / Nachverhandlung eines großen Teils der Verträge mit IKT-Drittdienstleistern notwendig.
2. Die Definition von vertraglichen Vereinbarungen zur Nutzung von IKT-Dienstleistungen ist weiter gefasst als die bisherigen Auslagerungsdefinitionen, es besteht Unsicherheit bei der Überführung und Abgrenzung.
3. Bisher sind Vorgaben der DORA zum Drittparteirisikomanagement und die Regulatorik im Bereich Auslagerungen nicht harmonisiert.
4. Die Anforderungen an Ausstiegsstrategien/-pläne steigen. Die bisherige Privilegierung von gruppen- oder verbundsinternen Auslagerungen entfällt, eine Berücksichtigung der Proportionalität ist aber weiterhin mit Bezug auf ein reduziertes Risiko (insoweit zutreffend) möglich.
5. Die Analyse der Konzentrationsrisiken im Finanzunternehmen hat zum Ziel diese zu ermitteln und angemessen zu überwachen.



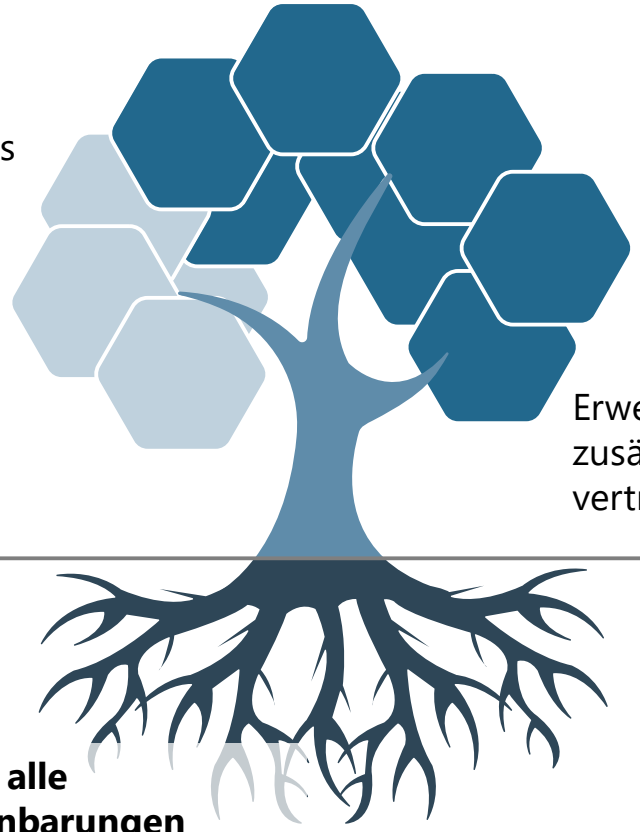
erwarteter Umsetzungsaufwand:
sehr hoch

Bei aktuell vollständiger Compliance mit der sektoralen Auslagerungsregulatorik sind einige der Anforderungen an das IKT-Drittparteirisikomanagement durch bestehende Strukturen für das Auslagerungsmanagement bereits abgedeckt. Herausfordernd wird allerdings die neue Einwertung der Dienstleistungsbezüge und die Verhandlung der neuen Vertragsklauseln sowie die Konkretisierung und das Testen von Ausstiegsplänen. Hinzu kommt die Erstellung eines neuen Informationsregisters.

Übersicht Vertragsanforderungen aus DORA

Anforderungen für vertragliche Vereinbarungen zu IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen (hauptsächlich Art. 30 Abs. 3 DORA)

Anforderungen aus den zwei IKT-Drittparteirisiko-RTSen



Erweiterte oder zusätzliche Mindest-vertragsinhalte

Anforderungen für alle vertraglichen Vereinbarungen (hauptsächlich Art. 30 Abs. 2 DORA)

Thema	alle	kritisch/wichtig
Anforderungen an die Form und Veränderung von vertraglichen Vereinbarungen	ja	erweitert
Beschreibung der Dienstleistung	ja	erweitert
Beschreibung der Dienstleistungsgüte	ja	erweitert
Unterauftragsvergabe	nein	ja
Standort	ja	ja
Datenschutz	ja	ja
Zugang zu Daten	ja	ja
IKT-Vorfallsunterstützung	ja	ja
Zusammenarbeit mit Aufsichtsbehörden	ja	ja
Prüfrechte / fortlaufende Überwachung	nein	ja
Kündigungsrechte und Fristen	ja	erweitert
Teilnahme an Schulungen des FU	ja	ja
Berichtspflichten	nein	ja
Notfallpläne	nein	ja
spezifische Maßnahmen zur IKT-Sicherheit	nein	ja
Beteiligung an TLPT	nein	ja
Ausstiegsstrategien	nein	ja

Ausgestaltung der Verträge abhängig von betroffener Funktion

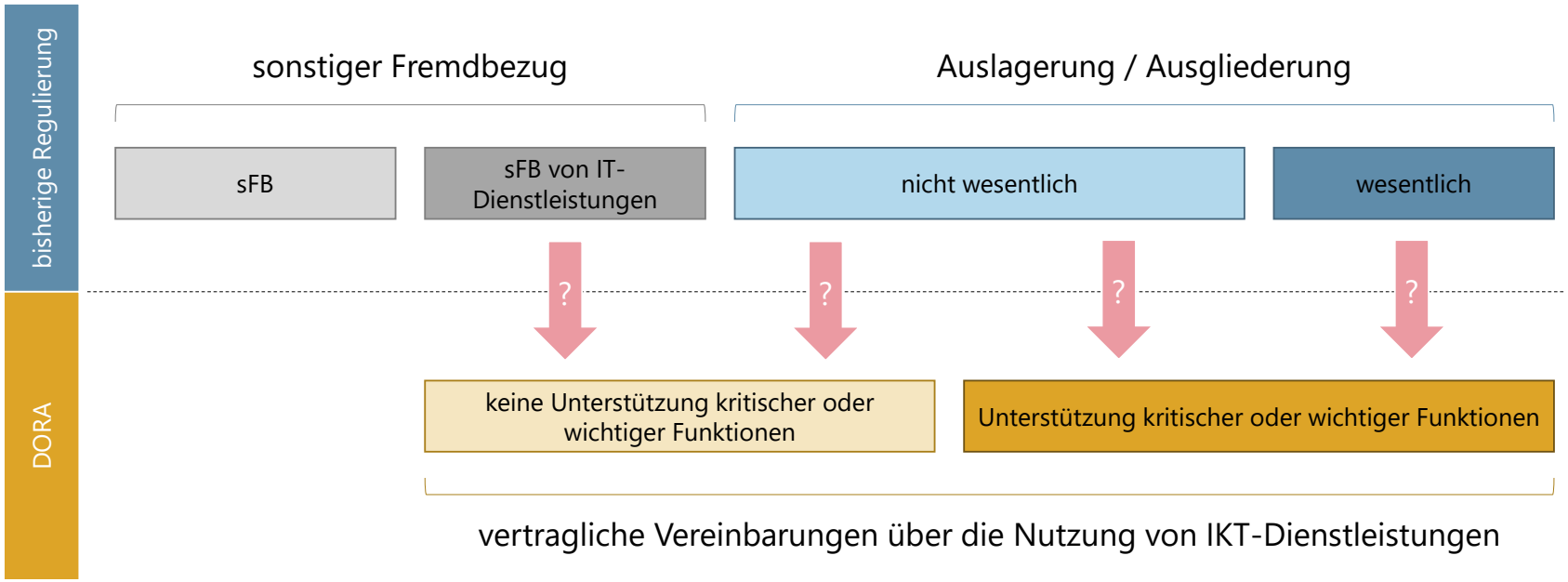
Unterscheidung zwischen IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen und solchen, die dies nicht tun als Grundlage. Erster Schritt ist somit eine entsprechende Bewertung der betroffenen Funktionen. Kriterien müssen dazu auf Basis der Definition in DORA (siehe RTS-E TPPol) entwickelt werden.

Definition (zusammengefasst):

Kritisch oder wichtig sind Funktionen, wenn ihr Ausfall eine erhebliche Beeinträchtigung

- der finanziellen Leistungsfähigkeit,
- der Geschäftsfortführung oder
- regulatorischer Art

darstellen würde.

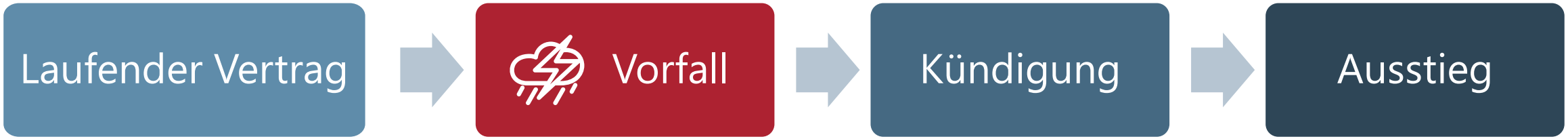


Klarheit von vertraglichen Vereinbarungen

Herausforderung:
häufig komplexe, unklare und unübersichtliche Verträge, insbesondere bei großen IKT-Drittdienstleistern oder bereits lang laufenden Vertragsbeziehungen

- § Vollständiger Vertrag in **einem Dokument** muss beiden Parteien in Papierform zur Verfügung stehen, alternativ in einem „herunterladbaren, dauerhaften und zugänglichen Format“ (Art. 30 Abs. 1 DORA).
- § **Klare und vollständige Beschreibung** aller IKT-Dienstleistungen und Funktionen, die durch den IKT-Drittdienstleister erbracht werden und Beschreibung der Dienstleistungsgüte (Art. 30 Abs. 2 lit. a und e DORA)
- § **Aktualisierungen und Überarbeitungen** der Beschreibungen der Dienstleistungsgüte müssen im Vertrag enthalten sein (Art. 30 Abs. 2 lit. e und Art. 30 Abs. 3 lit. a DORA).
- § **Wesentliche Änderungen** an der vertraglichen Vereinbarung müssen in einem schriftlichen Dokument, datiert und von allen Parteien unterschrieben sein (Art. 8 Abs. 4 RTS-E TPPol).

Vorsorge für den Fall der Fälle treffen



- Sicherstellung des Zugangs zu Daten (z.B. bei Insolvenz), Wiederherstellung und Rückgabe (Art. 30 Abs. 2 lit. d DORA)
- Teilnahme an Sensibilisierungen und Schulungen des Finanzunternehmens zu IKT-Sicherheit und digitaler operationalen Resilienz (Art. 30 Abs. 2 lit. i DORA)
- Implementierung und Test von Notfallplänen (Art. 30 Abs. 3 lit. c DORA)

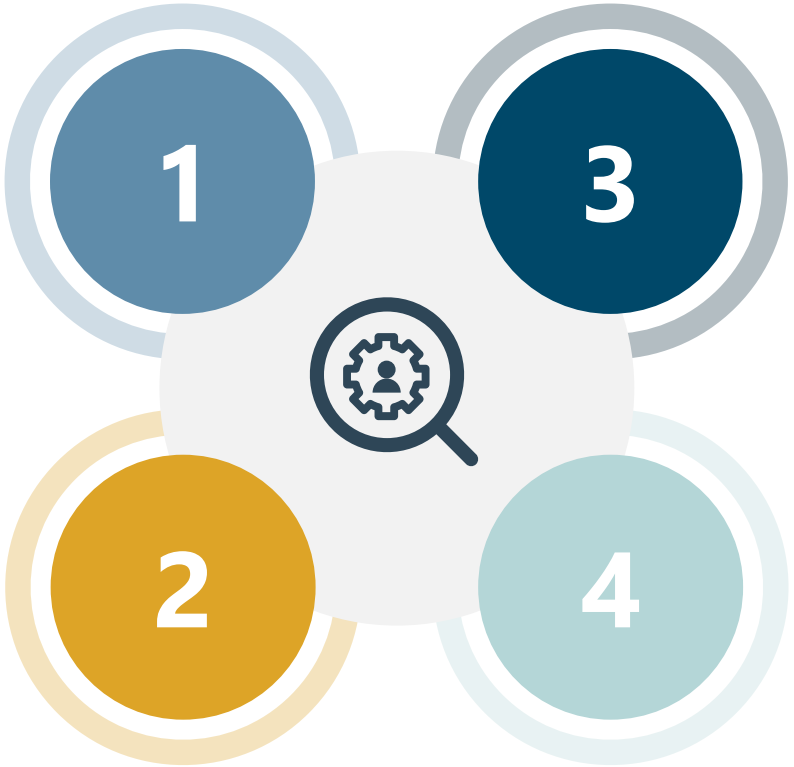
- Unterstützung bei einem IKT-Vorfall, Festsetzung der Kosten (Art. 30 Abs. 2 lit. f DORA)

- Kündigungsrechte bei Verstößen oder Schwächen des Dienstleisters (Art. 28 Abs. 7 DORA)
- Kündigungsrechte und Mindestkündigungs-fristen entsprechend den Erwartungen der zuständigen Behörden (Art. 30 Abs. 2 lit. h DORA)

- Ausstiegsstrategien und Festlegung eines verbindlichen angemessenen Übergangszeitraum (Art. 30 Abs. 3 lit. f DORA)

Effektive Prüfrechte für Finanzunternehmen

Recht zur fortlaufenden Überwachung der Leistung des IKT-Drittdienstleisters (Art. 30 Abs. 3 lit. e DORA)



Uneingeschränkte Zusammenarbeit bei Vor-Ort-Inspektionen und Audits (Art. 30 Abs. 3 lit. e (iii) DORA)

Prüfrechte für das Finanzunternehmen und die Aufsicht, inkl. dem Recht Kopien anzufertigen (Art. 30 Abs. 3 lit. e (i) DORA)

Prüfungs- und Testrechte (Art. 8 Abs. 2, Art. 8 Abs. 3 lit. g und h sowie Art. 3 Abs. 9 lit. c und d RTS-E TPPol)

Zulässige Einschränkung der Prüfrechte:

- bei Betroffenheit Rechte anderer Kunden, Vereinbarung „alternativer Bestätigungsniveaus“ (Art. 30 Abs. 3 lit. e (ii) DORA)
- Mitteilungspflicht zur Prüfungsplanung, d.h. Umfang und Häufigkeit (Art. 30 Abs. 3 lit. e (iv) DORA)
- Wahrnehmung der Prüfungsrechte durch unabhängigen Dritten bei Kleinstunternehmen, keine eigenen Prüfungen (Art. 30 Abs. 3 DORA)

Umfangreiche Vertragsklauseln zur Unterauftragsvergabe

- **Zulässigkeit Unterauftragsvergabe** („die kritische oder wichtige Funktionen oder wesentliche Teile davon unterstützen“) und **Bedingungen für die Unterauftragsvergabe** (Art. 30 Abs. 2 lit. a DORA)
- **Konkretisierung** der Beschreibung und Bedingungen, unter denen eine Unterauftragsvergabe zulässig ist (Art. 4 RTS-E SUB)
- Verpflichtung der **Nachbildung der relevanten Vertragsinhalte** bei Unterauftragsvergaben (Art. 3 Abs. 1 lit. c RTS-E SUB)
- **Ausreichende Mitteilungsfrist** bei wesentlichen Veränderungen bei Unterauftragsvergaben und Verpflichtung in dieser Frist keine Veränderungen zu vollziehen, sowie das Recht Änderungen zu verlangen (Art. 6 Abs. 1, 3 und 4 RTS-E SUB)
- **Kündigungsrecht,** wenn während der Frist oder ohne Zustimmung Veränderungen vollzogen werden (Art. 7 RTS-E SUB)

Hinweis:
Der RTS befindet sich aktuell noch in der Konsultation, daher können sich die Inhalte noch verändern.

Wird es Übergangsfristen geben?

- Bestehende Verträge müssen **nachverhandelt** werden, damit es zu einer Angleichung an die in DORA vorgesehenen Vertragsbestimmungen kommt, siehe dazu Erwägungsgrund 69 DORA: *„Bei der Neuaushandlung vertraglicher Vereinbarungen zwecks Angleichung an die Anforderungen dieser Verordnung sollten Finanzunternehmen und IKT-Drittdienstleister sicherstellen, dass die in dieser Verordnung vorgesehenen wesentlichen Vertragsbestimmungen berücksichtigt werden.“*

- Es sind **keine Übergangsfristen** für die Anpassung der bestehenden vertraglichen Vereinbarungen vorgesehen.

- Art. 3 Abs. 2 RTS-E TPPol weißt darauf hin, dass es einen dokumentierten Implementierungszeitplan geben und die Umsetzung rechtzeitig erfolgen soll. Die Anpassung der vertraglichen Vereinbarungen soll **so schnell wie möglich** vorgenommen werden.

- Es sollen bei Vertragsabschluss **Standardvertragsklauseln**, die von Behörden für bestimmte Dienstleistungen entwickelt wurden, berücksichtigt werden (Art. 30 Abs. 4 DORA). Aktuell liegen allerdings keine Standardvertragsklauseln vor, beaufsichtigte Unternehmen sollten daher nicht die Veröffentlichung von Standardvertragsklauseln zur Umsetzung der Mindestvertragsinhalte abwarten.

BaFin

Bundesanstalt für
Finanzdienstleistungsaufsicht

Pause

BaFin

Bundesanstalt für
Finanzdienstleistungsaufsicht

Virtuelle Fragerunde zu den vertraglichen Anforderungen an die Nutzung von IKT-Dienstleistungen

Dr. Sven Kleinknecht-Dennart

BaFin
Bundesanstalt für Finanzdienstleistungsaufsicht

Diese Präsentation sowie weitere Informationen zu DORA erhalten Sie auf www.bafin.de/dora !

Janusz Dreier

BaFin
Referat GIT 2, Incident Reporting, Überwachung IT-Mehrmandantendienstleister und Krisenprävention

E-Mail: janusz.dreier@bafin.de

Dr. Sibel Kocatepe

BaFin
Referat GIT 2, Incident Reporting, Überwachung IT-Mehrmandantendienstleister und Krisenprävention

E-Mail: sibel.kocatepe@bafin.de

Dr. Sven Kleinknecht-Dennart

BaFin
Referat GIT 3, Grundsatz IT-Aufsicht und Aufsichtsunterstützung

E-Mail: sven.kleinknecht-dennart@bafin.de