GÖRG

IHRE WIRTSCHAFTSKANZLEI

GÖRG
INSOLVENZVERWALTUNG

GÖRG
RECHTSANWÄLTE

BWLS
STEUERBERATUNG

GÖRG

IHRE WIRTSCHAFTSKANZLEI

AK Digitaler Zahlungsverkehr – Cyber Security im Zahlungsverkehr

Vorschlag der EU-Kommission eines Digital Operational Resilience Act

Dr. Matthias Terlau, Frankfurt am Main, 28. April 2022

DORA = Digital Operational Resilience Act
Zielrichtung

GÖRG
IHRE WIRTSCHAFTSKANZLEI

- Regulierung des Sicherheitsmanagements
- der Informations- und Kommunikationstechnologie (IKT)
- im Finanzsektor
- entlang der gesamten Wertschöpfungskette

Aktueller Stand des Verordnungsvorschlags

GÖRG
IHRE WIRTSCHAFTSKANZLEI

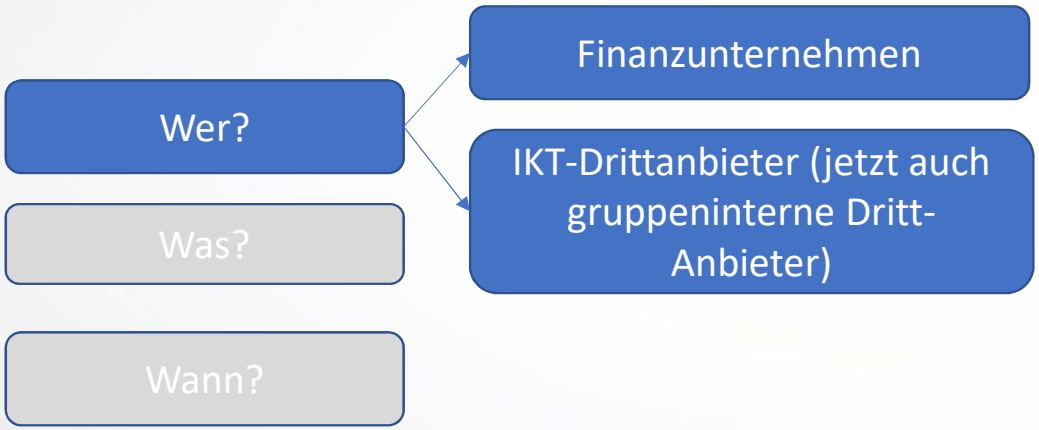
DORA – Ein Überblick

GÖRG
IHRE WIRTSCHAFTSKANZLEI

- Wer?
- Was?
- Wann?

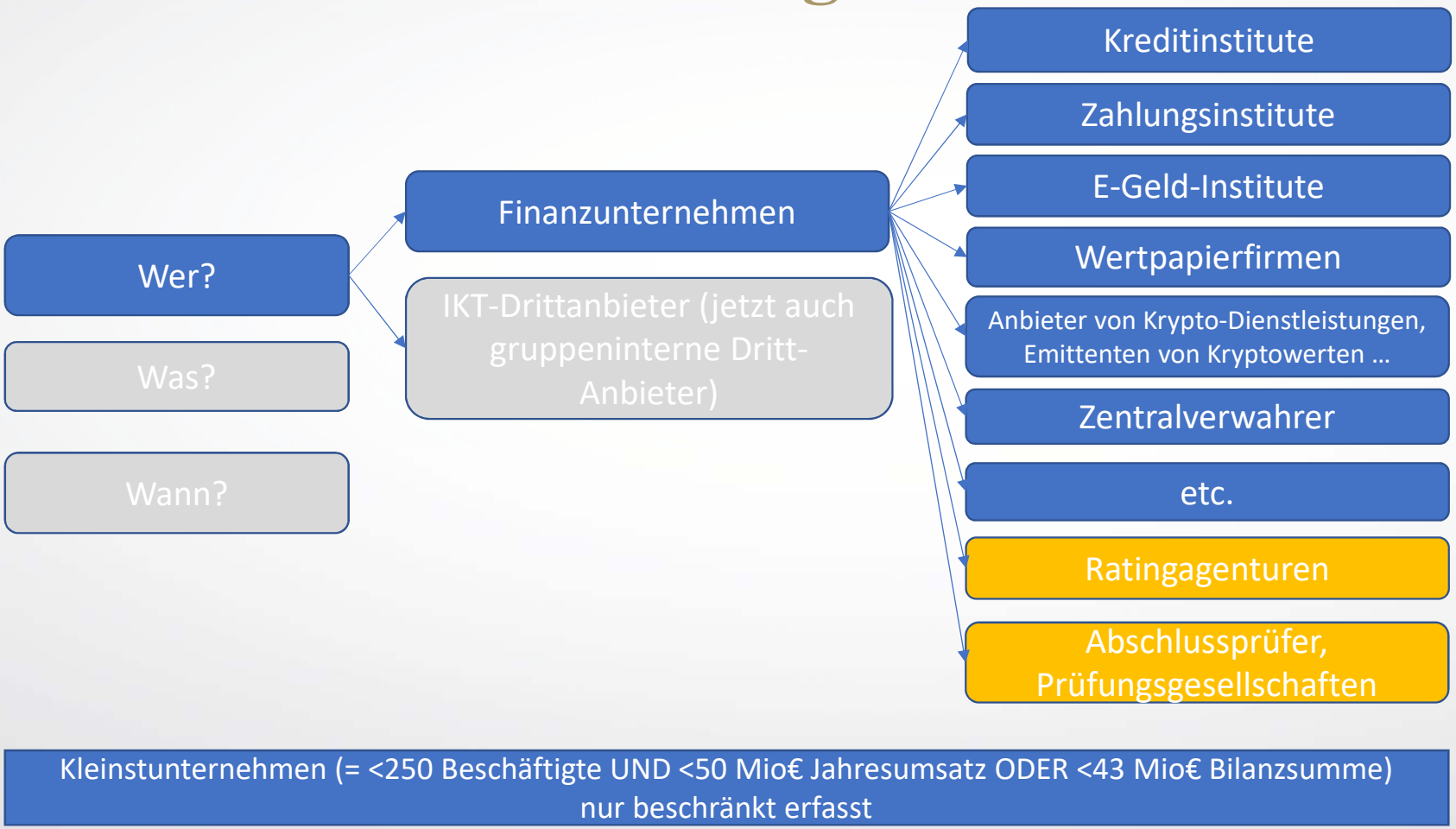
Persönlicher Anwendungsbereich

GÖRG
IHRE WIRTSCHAFTSKANZLEI



Persönlicher Anwendungsbereich

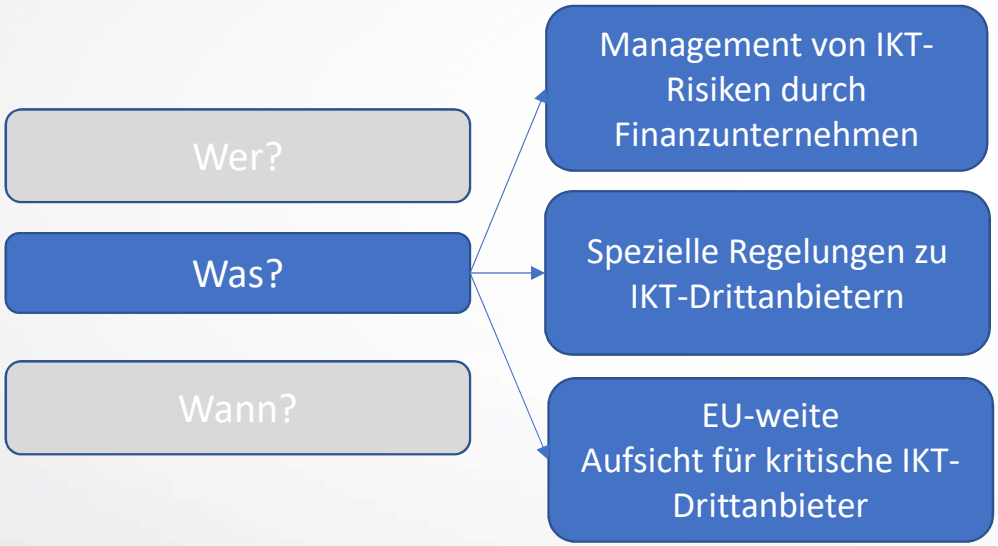
GÖRG
IHRE WIRTSCHAFTSKANZLEI



Kleinstunternehmen (= <250 Beschäftigte UND <50 Mio€ Jahresumsatz ODER <43 Mio€ Bilanzsumme) nur beschränkt erfasst

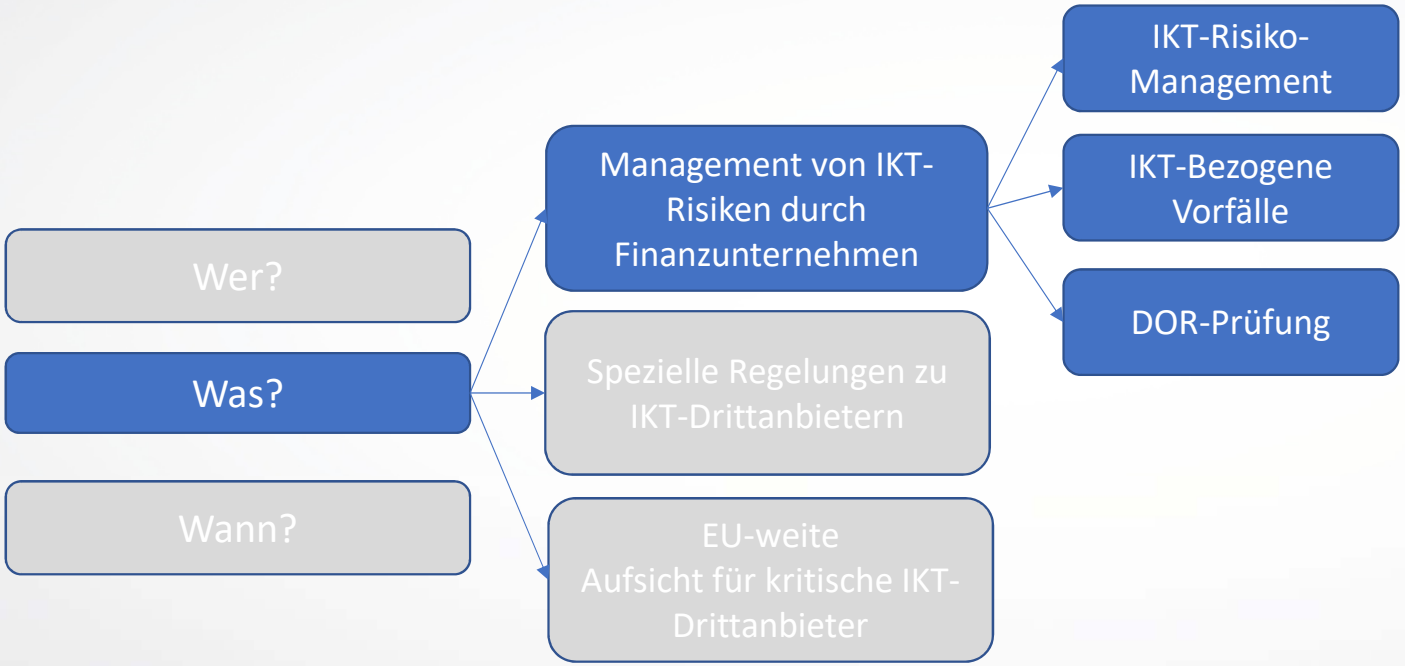
Die Regelungen im Überblick

GÖRG
IHRE WIRTSCHAFTSKANZLEI



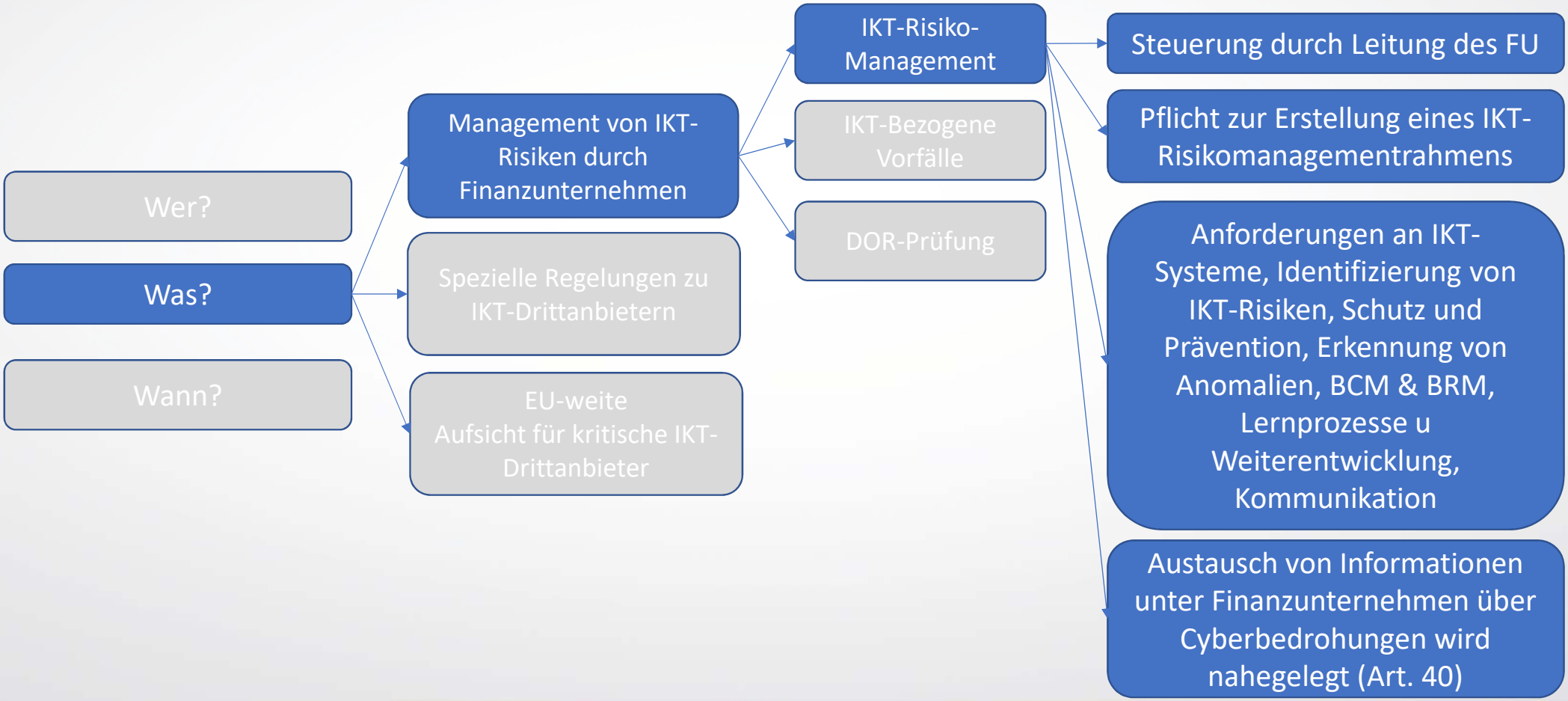
Die Regelungen im Überblick

GÖRG
IHRE WIRTSCHAFTSKANZLEI



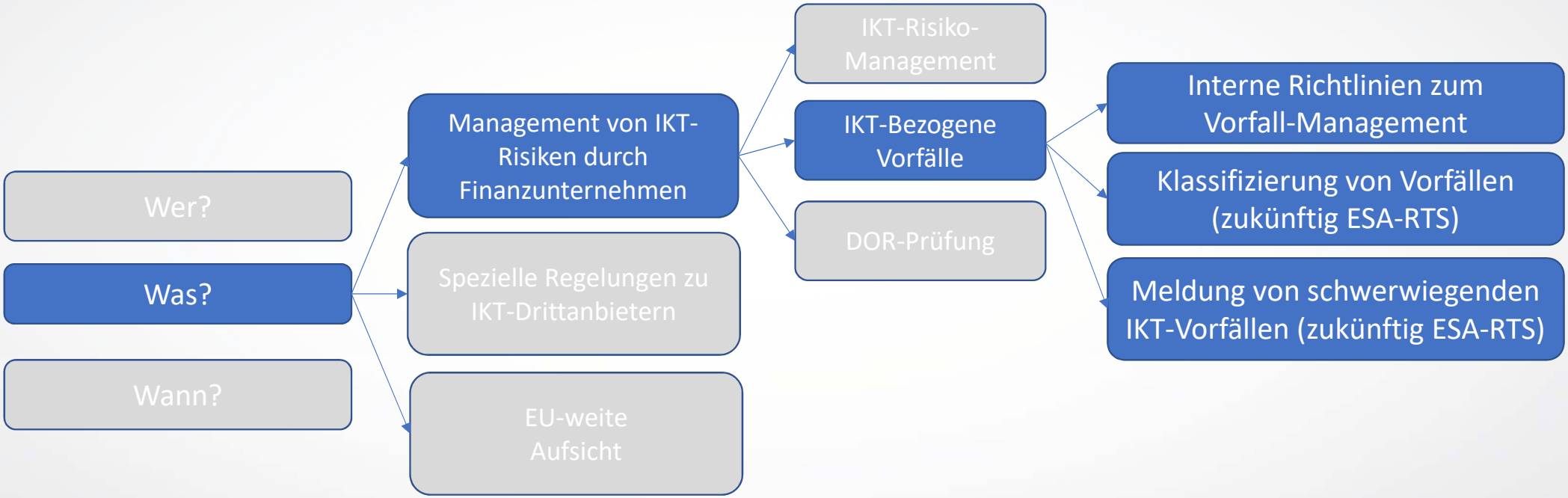
IKT-Risikomanagement

GÖRG
IHRE WIRTSCHAFTSKANZLEI



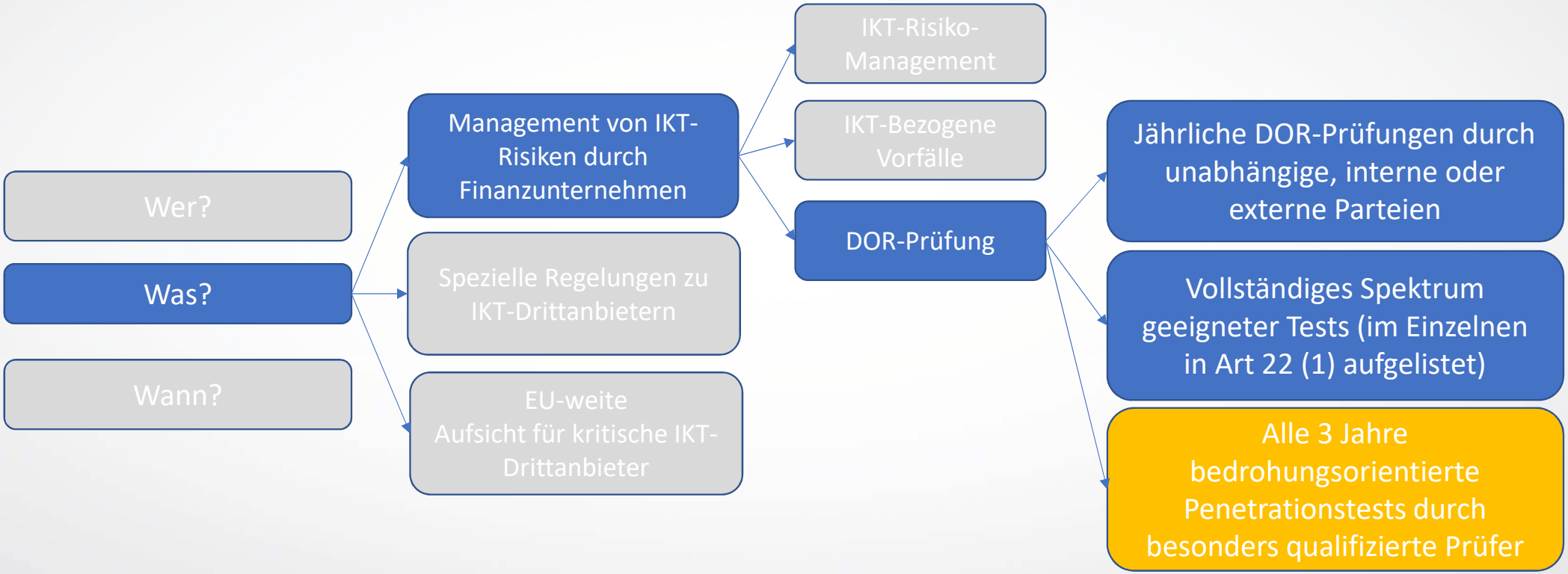
IKT-Bezogene Vorfälle

GÖRG
IHRE WIRTSCHAFTSKANZLEI



DOR-Prüfung

GÖRG
IHRE WIRTSCHAFTSKANZLEI



Bedrohungsorientierte Penetrationstests

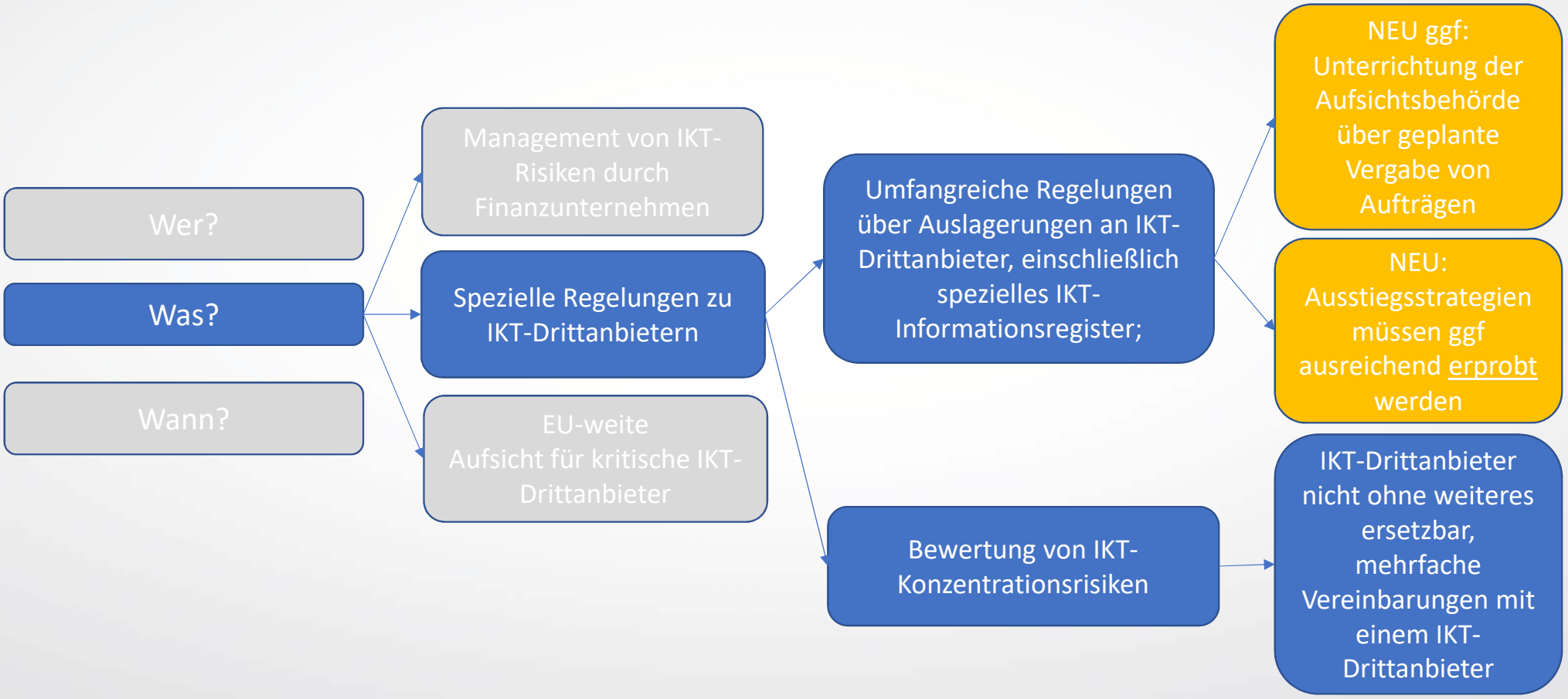
GÖRG
IHRE WIRTSCHAFTSKANZLEI

Bedrohungsorientierte Penetrationstests	Betroffene Finanzunternehmen	Anforderungen an Prüfer
Kritische Funktionen und Dienstleistungen	Aufsichtsbehörde wählt aus	Interne und externe Prüfer
An Live-Produktionssystemen	Maßstab: Kritikalität der Dienstleistungen	Besondere Eignung und Zuverlässigkeit sowie Zertifizierung für derartige Penetrationstests sind vorher nachzuweisen
zugrunde liegende IKT-Systeme, -Systeme und -Technologien	Maßstab: Bedenken hinsichtlich Finanzstabilität	
einschließlich an IKT-Drittanbieter ausgelagerte Funktionen	Maßstab: IKT-Risikoprofil, IKT-Reifegrad	
Bericht an Aufsichtsbehörde		Zukünftig weitere Präzisierungen in RTS der EBA, ESMA, EIOPA

„bedrohungsorientierte Penetrationstests“ bezeichnet einen Rahmen, der Taktik, Techniken und Verfahren realer Angriffsvektoren, die als echte Cyberbedrohung empfunden werden, nachbildet und einen kontrollierten, maßgeschneiderten, erkenntnisgestützten (Red-Team-)Test der kritischen Live-Produktionssysteme des Unternehmens ermöglicht;

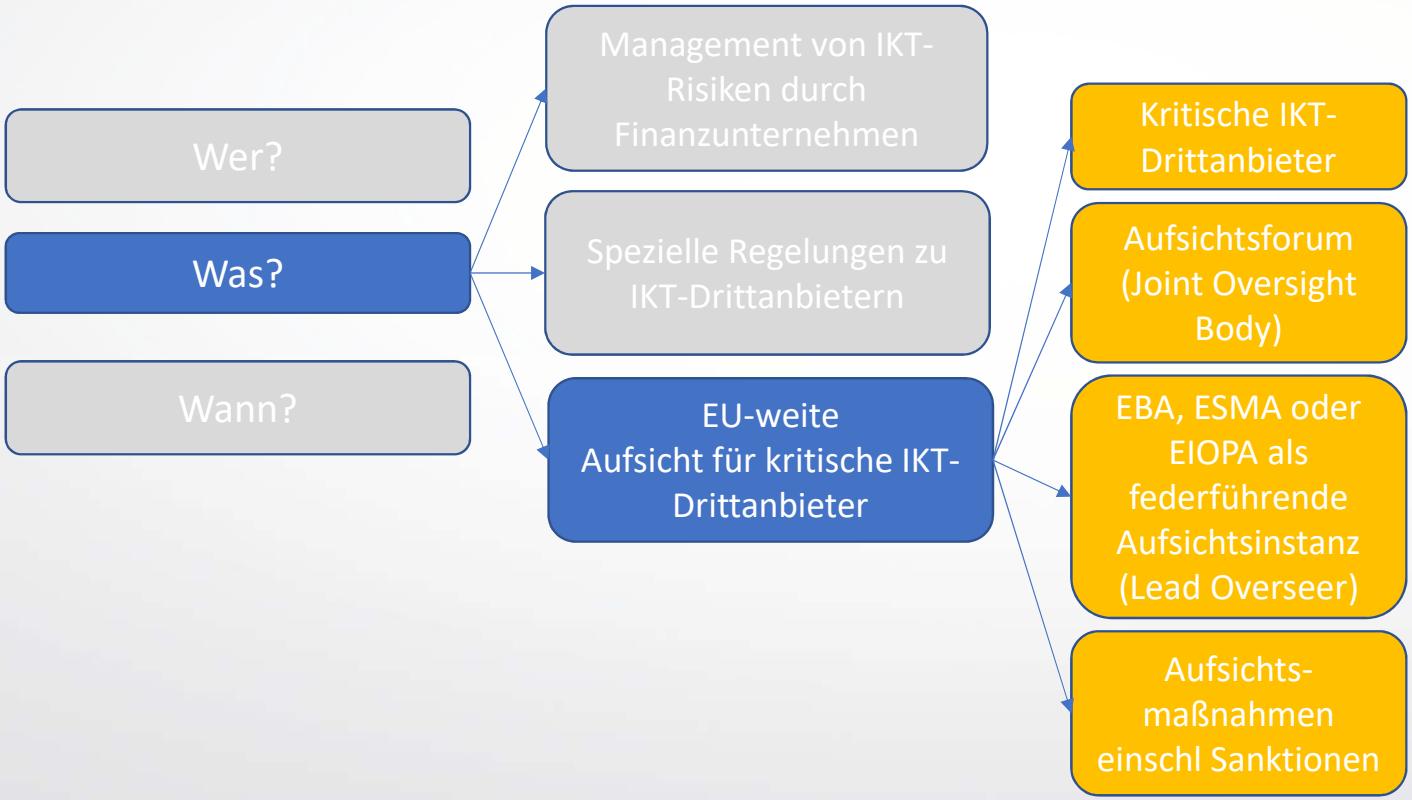
Auslagerung an IKT-Drittanbieter

GÖRG
IHRE WIRTSCHAFTSKANZLEI



GÖRG
IHRE WIRTSCHAFTSKANZLEI

EU-weite Aufsicht über kritische IKT-Drittanbieter



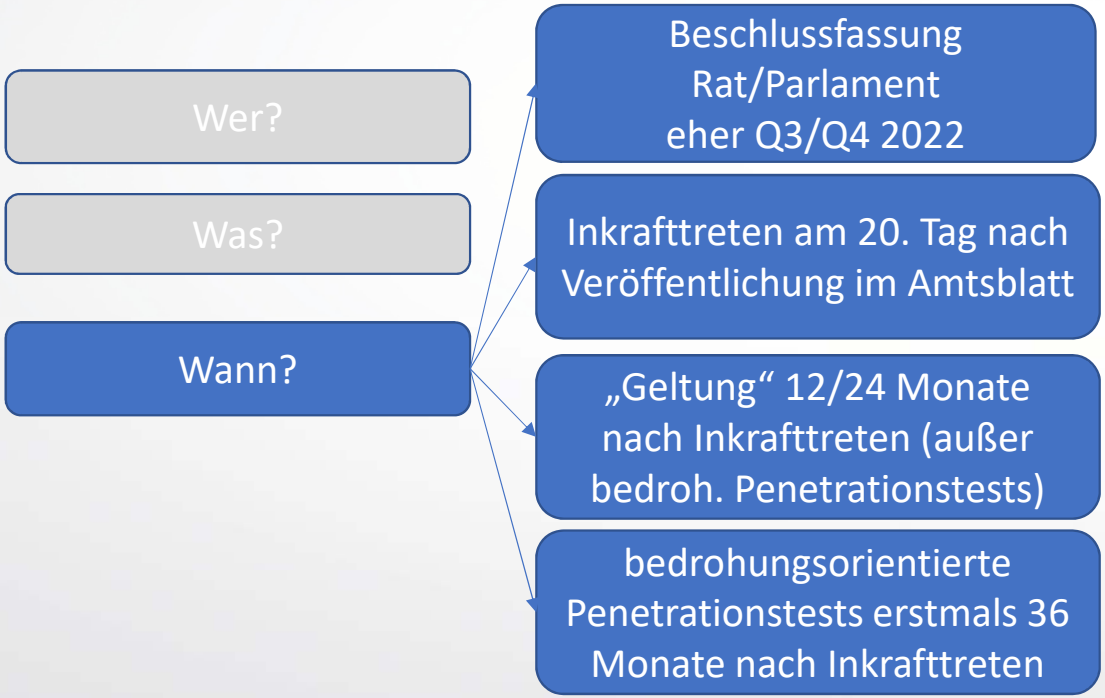
EU-weite Aufsicht über kritische IKT-Drittanbieter

GÖRG
IHRE WIRTSCHAFTSKANZLEI

Kriterien für Kritische IKT-Drittanbieter	Lead Overseer	Aufsichtsmaßnahmen
Umfassende Betriebsstörung hätte **systemische Auswirkungen**	**Umfassende Prüfung des IKT-Risikomanagements bei jedem kritischen IKT-Drittanbieter**	Umfassende **Informations-, Prüfungs-, Untersuchungs-, Inspektionsrechte** des Lead Overseer
Systemischer Charakter u Bedeutung der angeschlossenen Finanzunternehmen	Lead Overseer (Rat: zust. ist Joint Oversight Body) verabschiedet **individuellen Aufsichtsplan** für jeden einzelnen kritischen IKT-Drittanbieter	Befugnis zur Verhängung von **Zwangsgeld**
Abhängigkeit der Finanzunternehmen	**Beschränkung der nationalen Aufsichtsbehörden** durch Aufsichtsplan; Abstimmung mit Lead Overseer verpflichtend	Nach Abstimmung mit Joint Oversight Body **Empfehlungen** an den kritischen IKT-Drittanbieter (wird auch mit nat. Aufsichtsbeh. [und FU?] geteilt)
Substituierbarkeit des IKT-Drittanbieters		Untersuchungen und Inspektionen durch **Joint Examination Team** (10 Personen) aus Lead Overseer und den zust nat. Aufsichtsbehörden
Zukünftig AusführungsVO der Kommission zur Präzisierung		
Liste wird veröffentlicht		

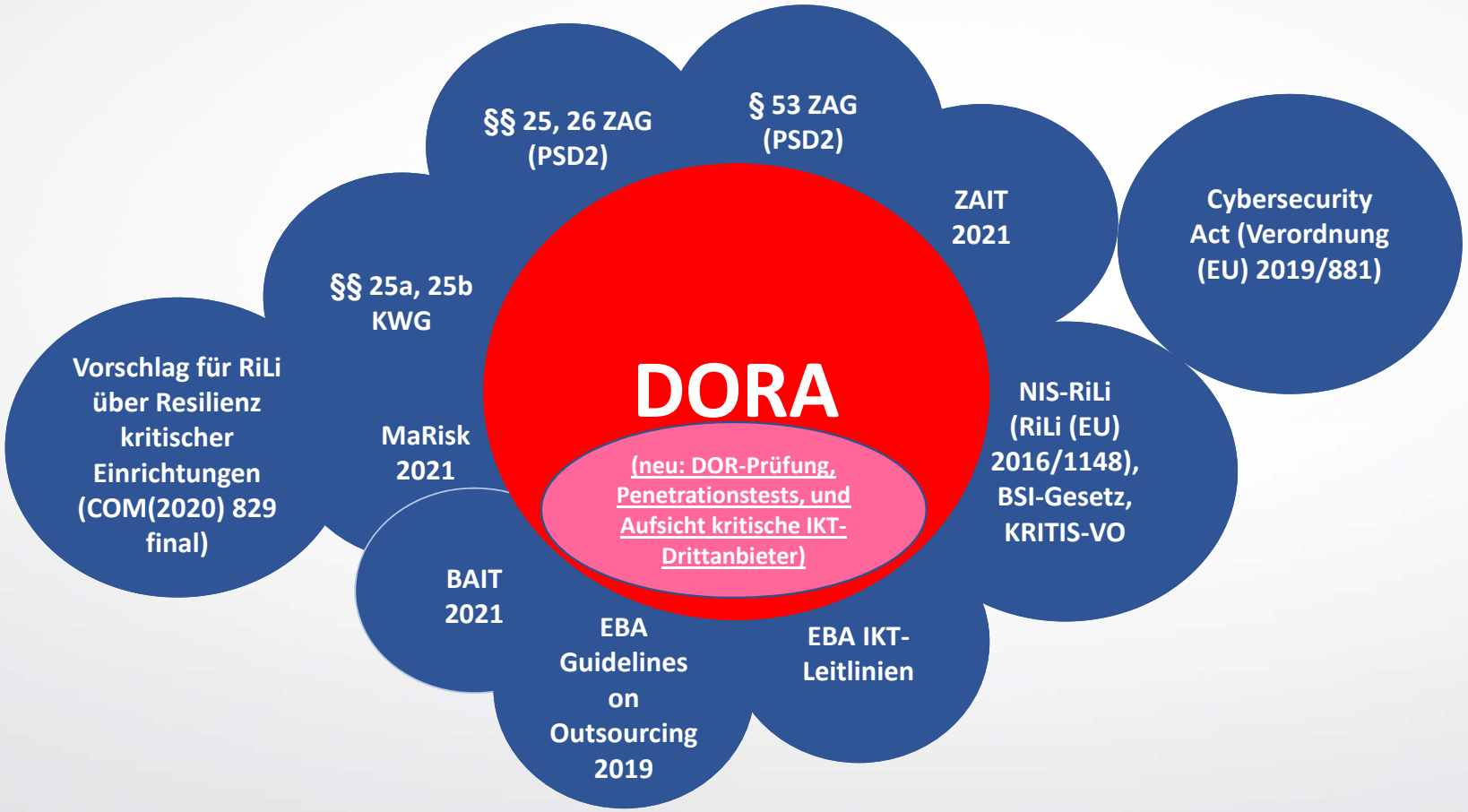
Zeitliche Anwendung

GÖRG
IHRE WIRTSCHAFTSKANZLEI



DORA für Zahlungsdienstleister (Kreditinstitute, Zahlungsinstitute, E-Geld-Institute) im Kontext

GÖRG
IHRE WIRTSCHAFTSKANZLEI



GÖRG
IHRE WIRTSCHAFTSKANZLEI

Vielen Dank für Ihre Aufmerksamkeit

weitere Informationen
unter payment-law.eu

Dr. Matthias Terlau

Kennedyplatz 2
50679 Köln
T: +49 221 33660-470
F: +49 221 33660-960
M: mterlau@goerg.de