

**DORA in der Praxis**  
Erfahrungen und Erkenntnisse  
nach dem Go-Live





## **Deloitte.**

**Nico Hass**  
Director  
Audit & Assurance

**Deloitte GmbH**  
Wirtschaftsprüfungsgesellschaft  
Europa-Allee 91  
60486 Frankfurt am Main  
Germany

Telefon: +49 (0)69 75695 6461  
Mobil: +49 (0)15 158005318  
nihass@deloitte.de

[www.deloitte.com/de](http://www.deloitte.com/de)

## **Deloitte.**

**Daniel Wittmann**  
Senior Manager  
Audit & Assurance

**Deloitte GmbH**  
Wirtschaftsprüfungsgesellschaft  
Europa-Allee 91  
60486 Frankfurt am Main  
Germany

Telefon: +49 (0)69 7569 57397  
Mobil: +49 (0)151 11622258  
dwittmann@deloitte.de

[www.deloitte.com/de](http://www.deloitte.com/de)

**Deloitte.**

**DORA Allgemein**  
Struktur



# DORA Allgemein

## Die fünf primären Handlungsfelder von DORA



**Deloitte.**

# IKT-Risikomanagement Struktur & Herausforderungen



# DORA Kapitel II IKT-Risikomanagement

## Artikel 5 – Artikel 16

### Artikel 5

#### Governance und Organisation

- Einrichtung eines Governance- und Kontrollrahmens und Einrichtung und Einbindung einer **Kontrollfunktion** für das IKT-Risikomanagement

### Artikel 6

#### IKT-Risikomanagementrahmen

- Einrichtung eines **IKT-Risikomanagementrahmens** als Teil des Gesamtrisikomanagementsystems

### Artikel 7

#### IKT-Systeme, -Protokolle und -Tools

- IKT-Systeme, -Protokolle und -Tools sind auf dem **neuesten Stand** zu halten

### Artikel 8

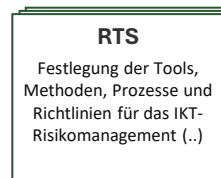
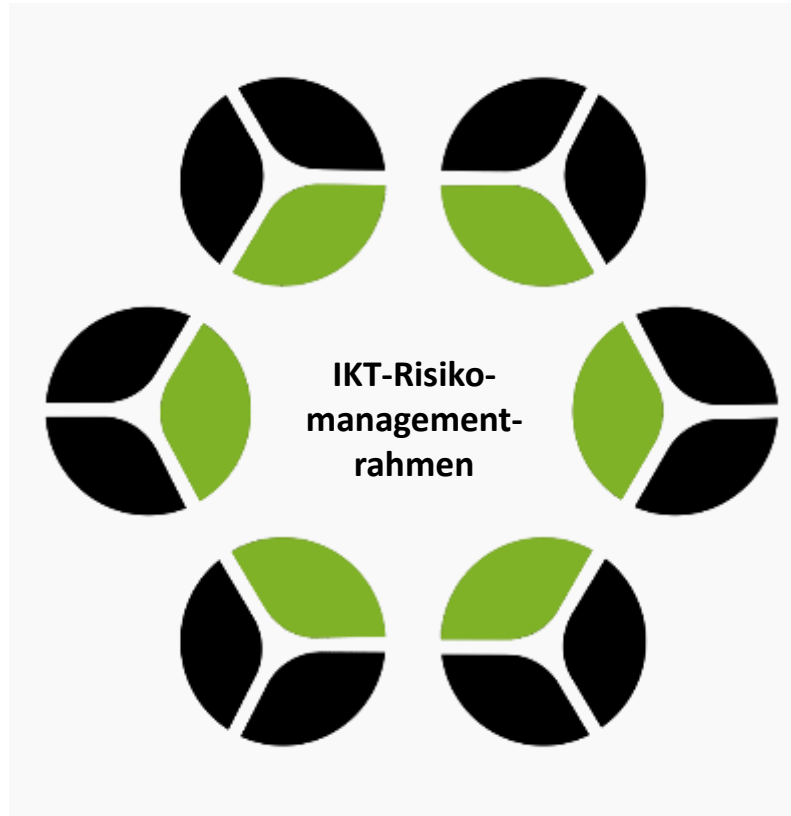
#### Identifizierung

- Identifikation und Dokumentation aller **IKT-Funktionen**, Rollen, Verantwortlichkeiten sowie **Informations-** und **IKT-Assets**

### Artikel 9

#### Schutz und Prävention

- Kontinuierliche **Überwachung** der Sicherheit und des Funktionierens der IKT-Systeme und -Tools und Einsatz angemessener risikomitigierender Maßnahmen



### Artikel 10

#### Erkennung

- Operationalisierung von Mechanismen zur Erkennung **anomalier Aktivitäten** und potenzieller Schwachstellen

### Artikel 11

#### Reaktion und Wiederherstellung

- Festlegung und Implementierung einer **(IKT-) Geschäftsfortführungsleitlinie** als Teil des IKT-Risikomanagementrahmens

### Artikel 12

#### Backup, Wiedergewinnung und Wiederherstellung

- Definition von Richtlinien und Verfahren für die **Datensicherung** sowie Wiedergewinnungs- und Wiederherstellungsverfahren.

### Artikel 13

#### Lernprozesse und Weiterentwicklung

- Bereitstellung von Kapazitäten und Personal, um **Informationen** über insbesondere IKT-bezogene Vorfälle und Cyberangriffe, zu **sammeln** und zu **analysieren**.

### Artikel 14

#### Kommunikation

- Festlegung von **Kommunikationsplänen** in Bezug auf IKT-bezogene Vorfälle und Cyberbedrohungen.

### Artikel 15 Anforderung an ESA

### Artikel 16 Vereinfachter IKT-Risikomanagementrahmen

# DORA Kapitel II IKT-Risikomanagement

## Herausforderungen, Erfahrungen und Erkenntnisse

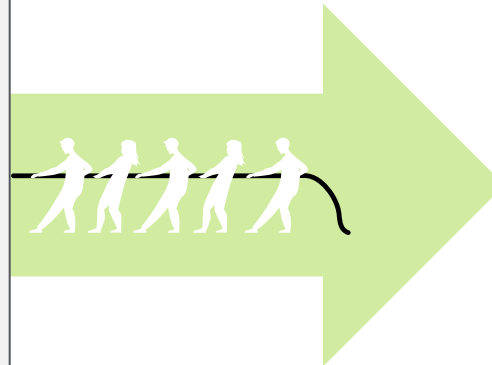
### Herausforderungen

#### Kritische oder wichtige Funktionen

- Die Identifikation kritischer oder wichtiger Funktionen (kwF) erfordert einen Überblick über den Informationsverbund
- Eine sauber modellierte und gepflegte Geschäftsprozesslandkarte und konsistente Klassifizierungen (SBK, BIA) sind von besonderer Bedeutung
- Veränderungen, z.B. in der BIA, können zu Verschiebungen der kwF-Systematik mit weitreichenden Auswirkungen führen
- Klärung des Umgangs mit querschnittlich genutzten Software- / Hardwarekomponenten

#### Datenhaltung

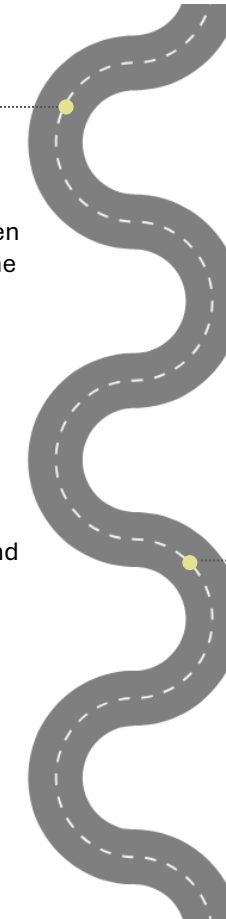
- Unzureichende Transparenz über vorhandene Daten und Datenflüsse
- Fehlende und unzureichende Mechanismen zur sicheren, nachvollziehbaren und resilienten Datenhaltung
- Dezentrale Datenhaltung erfordert die Implementierung vieler neuer Schnittstellen
- Datenqualität in dezentralen Datenszenen häufig mangelhaft



### Erfahrungen & Erkenntnisse

#### Kritische/wichtige Funktionen

- kwF-Systematik baut auf bestehenden Klassifizierungen deterministisch auf (Probleme werden an der Wurzel gelöst)
- Veränderungen der Klassifizierungen sollten automatisiert abgebildet werden und Folgeaktivitäten triggern
- Horizontale Vererbung sollte fallbezogen, wo sinnvoll, in Abstimmung zwischen 1st und 2nd LoD erfolgen

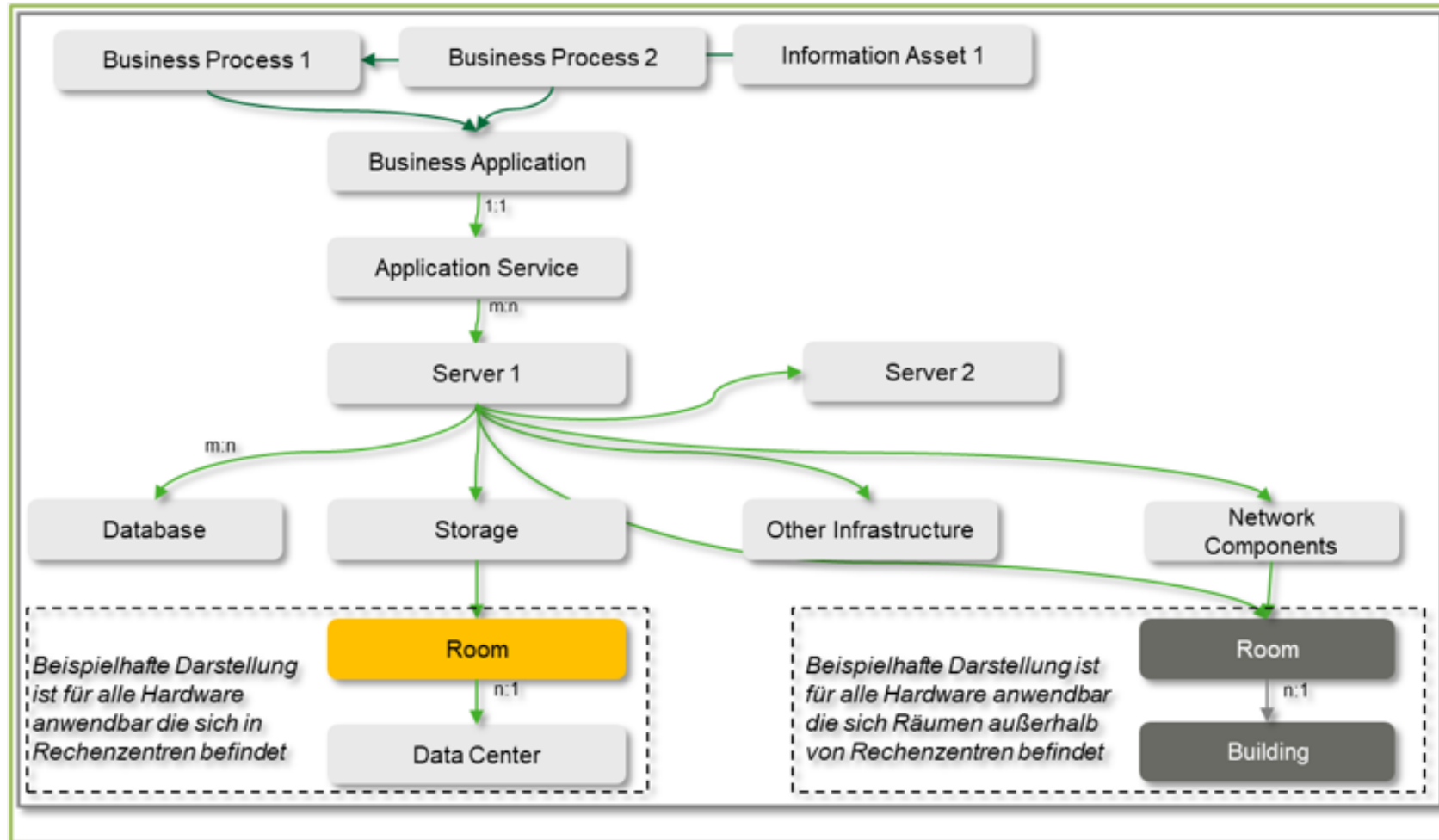


#### Datenhaltung

- Überblick über Daten- und Datenflüsse herstellen
- Datenqualität an der Quelle sicherstellen und durch geeignete Kontrollen überwachen
- Integration in zentrale Lösung (z.B. Data-Ware-House) förderlich

# DORA Kapitel II IKT-Risikomanagement

## Deep Dive: Modellierung von Prozessen und IKT-Assets



**Deloitte.**

# IKT-bezogene Vorfälle Struktur & Herausforderungen



# DORA Kapitel III Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle

## DORA Artikel 17 – Artikel 23

### Artikel 17

#### Prozess für die Behandlung IKT-bezogener Vorfälle

- Definition und Implementierung von Verfahren und Prozessen zur **Erfassung** aller IKT-bezogener Vorfälle und erheblicher Cyberbedrohungen
- Einrichtung und Implementierung eines Prozesses für die **Behandlung** IKT-bezogener Vorfälle und Vorgabe entsprechender Mindestinhalte
- Einrichtung von Verfahren und Prozessen zur **Mitigation, Ursachenermittlung, Dokumentation** und Ableitung angemessener **Maßnahmen**

### Artikel 18

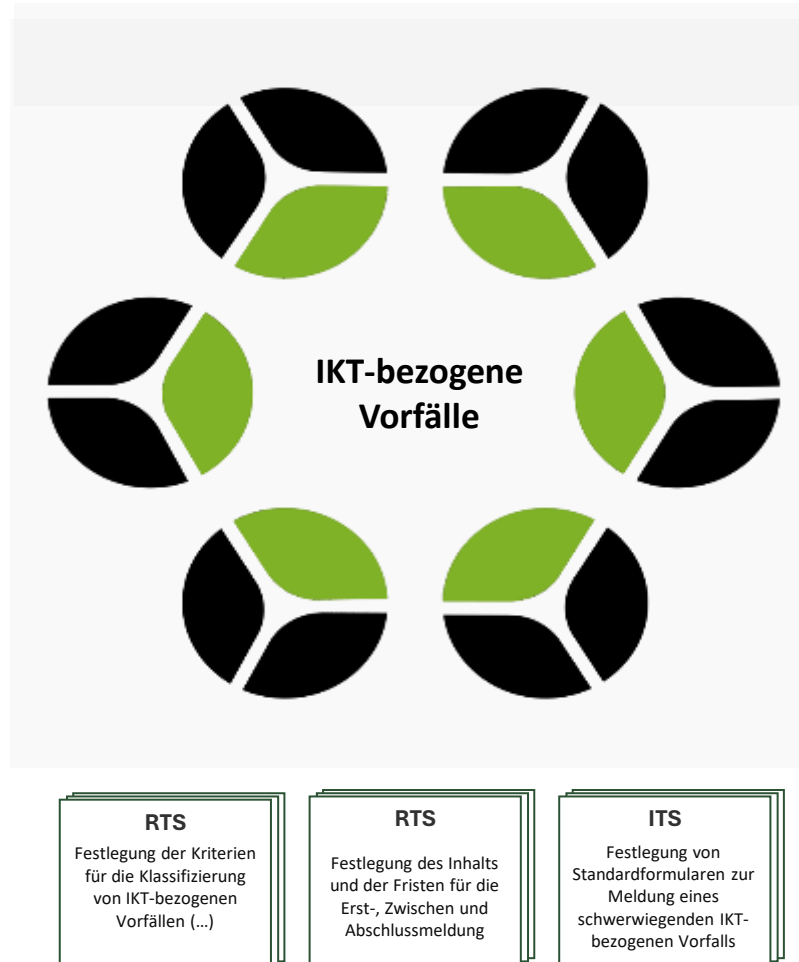
#### Klassifizierung von IKT-bezogenen Vorfällen und Cyberbedrohungen

- Vorgabe von **Kriterien** zur **Klassifikation** (schwerwiegender) IKT-bezogener Vorfälle und (erheblicher) Cyberbedrohungen unter Berücksichtigung der Vorgaben des RTS

### Artikel 19

#### Meldung schwerwiegender IKT-bezogener Vorfälle und freiwillige Meldung erheblicher Cyberbedrohungen

- Vorgabe zur **Meldung** schwerwiegender IKT-bezogener Vorfälle bei der zuständigen Behörde unter Berücksichtigung der RTS/ITS
- Verpflichtung zur unverzüglichen **Kundenkommunikation** bei Auftreten schwerwiegender IKT-bezogener Vorfälle mit Auswirkungen für die finanziellen Interessen der Kunden



### Artikel 20

#### Harmonisierung von Inhalt und Vorlagen von Meldungen

- Anforderung an ESA zur Erarbeitung und Abstimmung von harmonisierten Templates

### Artikel 21

#### Zentralisierung der Berichterstattung über schwerwiegende IKT-bezogene Vorfälle

- Einrichtung einer einheitlichen EU-Plattform für die Meldung schwerwiegender IKT-bezogener Vorfälle

### Artikel 22

#### Rückmeldungen von Aufsichtsbehörden

- Anforderungen an BaFin zur Bestätigung der Meldungen
- Nach Möglichkeit Bereitstellung von anonymisierten Informationen und Erkenntnisse zu ähnlichen Bedrohungen, angewandte Abhilfemaßnahmen und Möglichkeiten zur Eindämmung sektorweiter Auswirkungen

### Artikel 23

#### Zahlungsbezogene Betriebs- oder Sicherheitsvorfälle

- Anwendung der Anforderungen aus Kapitel III auch auf zahlungsbezogene Betriebs- oder Sicherheitsvorfälle (kein IKT-Bezug)

# DORA Kapitel III Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle

## Herausforderungen, Erfahrungen und Erkenntnisse

### Herausforderungen

#### Daten und Fristen

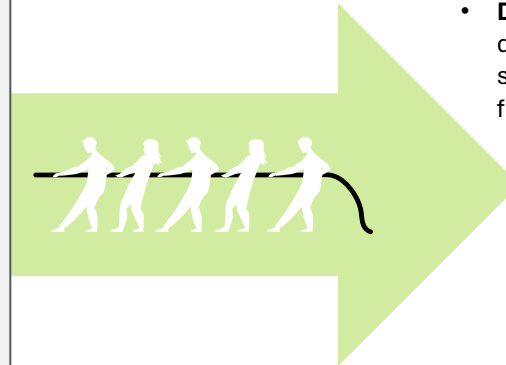
- Fristgerechte Bereitstellung der relevanten Daten, um Klassifizierung vorzunehmen, da häufig Stakeholder verschiedener Bereiche zuliefern müssen

#### Interpretationsspielraum

- Interpretationsbedürftige Begrifflichkeiten als Herausforderung und Chance zugleich

#### Betroffenheit und Informationspflichten

- Mapping zwischen Funktionen und betroffenen Kunden, um bspw. Informationspflichten nachzukommen



### Erfahrungen & Erkenntnisse

#### Daten und Fristen

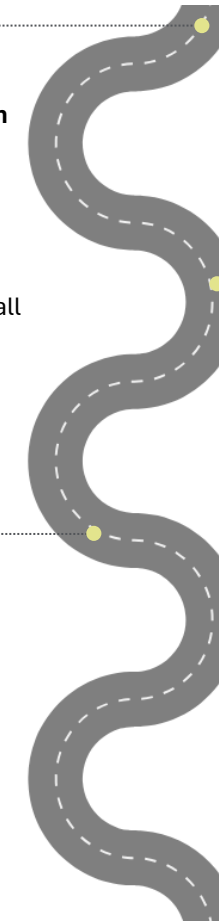
- Frühzeitige **Definition** relevanter **Datenquellen** und **Ansprechpersonen**
- **Strukturierte Datenaufbereitung** für die Klassifizierung/den Meldeprozess (inkl. der Schwellwerte)
- **Dry Run** für die „Konstellationen“ durchführen, die zu einem schwerwiegenden IKT-bezogenen Vorfall führen können

#### Betroffenheit und Informationspflichten

- Klar definierte Rollen und Verantwortlichkeiten
- Proaktiv Informationen über Kunden bereithalten (unter Beachtung der Datenschutzerfordernungen)

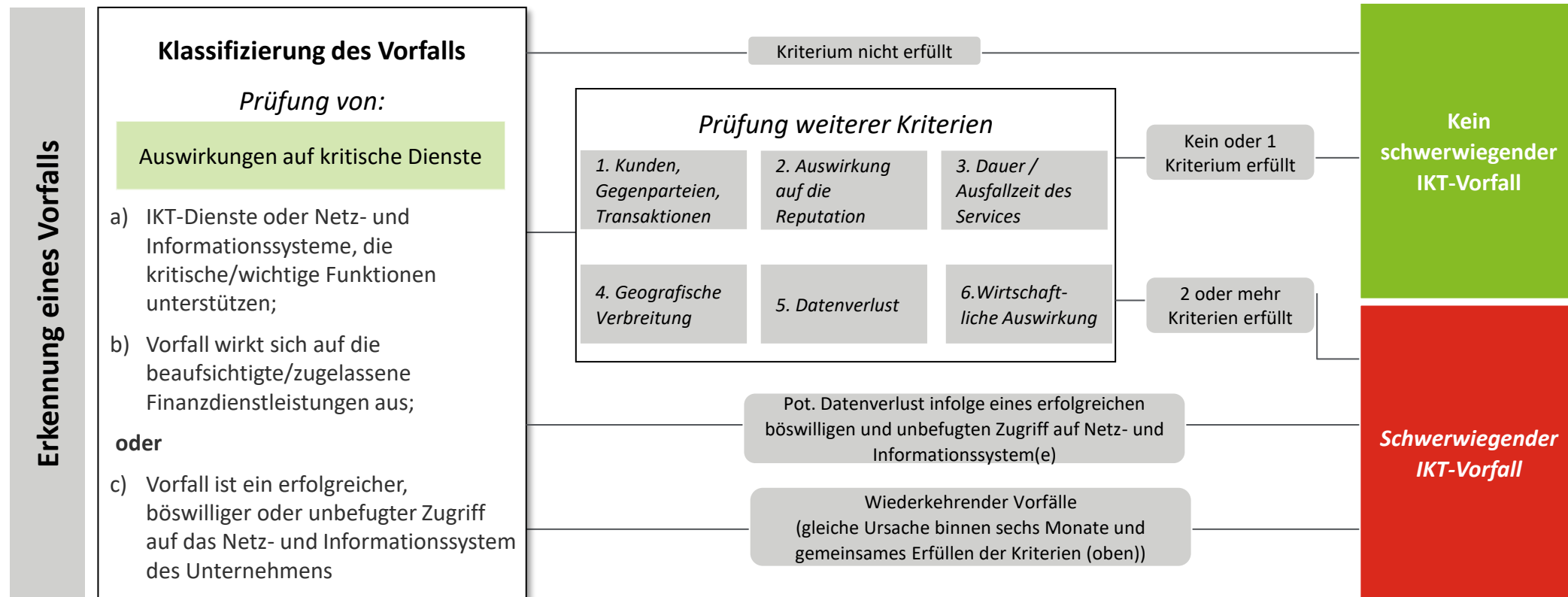
#### Interpretationsspielraum

- Gezielte **Schulung** der Mitarbeitenden zu IKT-Vorfallprozessen auch in den Fachbereichen
- Pragmatische und sinnvolle Definition wählen



# DORA Kapitel III Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle

## Deep-Dive: Daten und Fristen - Klassifizierung von IKT-bezogenen Vorfällen



**Deloitte.**

**Testen der digitalen operationalen Resilienz  
Struktur & Herausforderungen**



# DORA Kapitel IV Testen der digitalen operationalen Resilienz

## Artikel 24 – Artikel 27

### Artikel 24

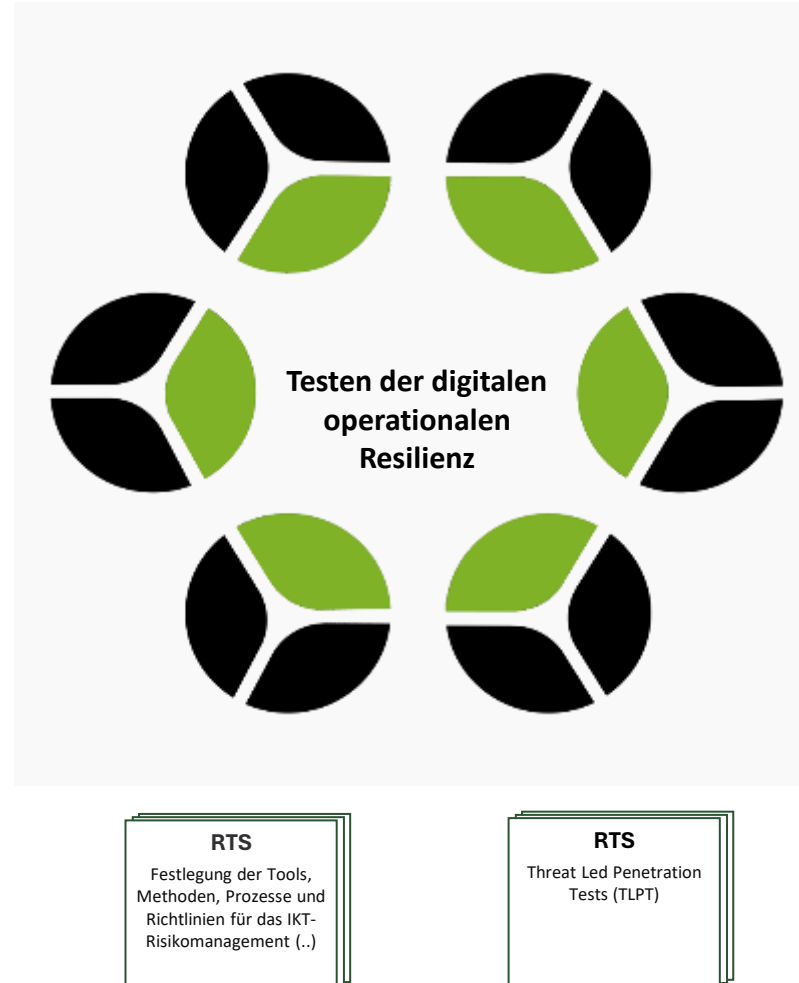
#### Allgemeine Anforderungen für das Testen der digitalen operationalen Resilienz

- Definition eines umfassenden und risikobasierten **Programms** für das **Testen** der **digitalen operationalen Resilienz** innerhalb des IKT-Risikomanagementrahmens
- Vorgabe und Implementierung von Bewertungen, Tests, Methoden, Verfahren und Tools gemäß Artikeln 25 und 26
- Gewährleistung der **Unabhängigkeit** der internen oder externen Tester
- Definition von Verfahren und Leitlinien zur Priorisierung, Klassifizierung und **Behebung** aller während der Durchführung der Tests identifizierter Probleme
- Mindestens jährliches Testen der IKT-Systeme und IKT-Anwendungen, die **kritische** oder **wichtige Funktionen** unterstützen

### Artikel 25

#### Testen von IKT-Tools und -Systemen

- Berücksichtigung des Grundsatzes der **Verhältnismäßigkeit** (Größe/Gesamtrisikoprofil) bei der Festlegung des Programms für die Tests der digitalen operationalen Resilienz
- Beispiele sind: Schwachstellenbewertung und -scans, Open-Source-Analysen, Netzwerksicherheitsbewertungen, Lückenanalysen, Überprüfungen der physischen Sicherheit, Fragebögen und Scans von Softwarelösungen, Quellcodeprüfungen soweit durchführbar, szenariobasierte Tests, Kompatibilitätstests, Leistungstests, End-to-End-Tests und Penetrationstests



### Artikel 26

#### Erweiterte Tests von IKT-Tools, -Systemen und -Prozessen auf Basis von TLPT (Threat-led Penetration Testing)

- Die zuständigen Behörden ermitteln Finanzunternehmen, die TLPT durchzuführen haben, spezifizierende Vorgaben hierzu finden sich im RTS JC 2024 29
- Zum aktuellen Zeitpunkt ergibt sich für die meisten Finanzunternehmen **keine Verpflichtung** zur **Durchführung von TLPTs**

### Artikel 27

#### Anforderungen an Tester bezüglich der Durchführung von TLPT

- Anforderungen an **Eignung** und Ansehen an **Tester**, die TLPT durchführen, insbesondere wenn es sich dabei um Mitarbeiter des Finanzinstituts handelt
- Regelungen zur vertraglichen Ausgestaltung des Einsatzes externer Tester

# DORA Kapitel IV Testen der digitalen operationalen Resilienz

## Herausforderungen, Erfahrungen und Erkenntnisse

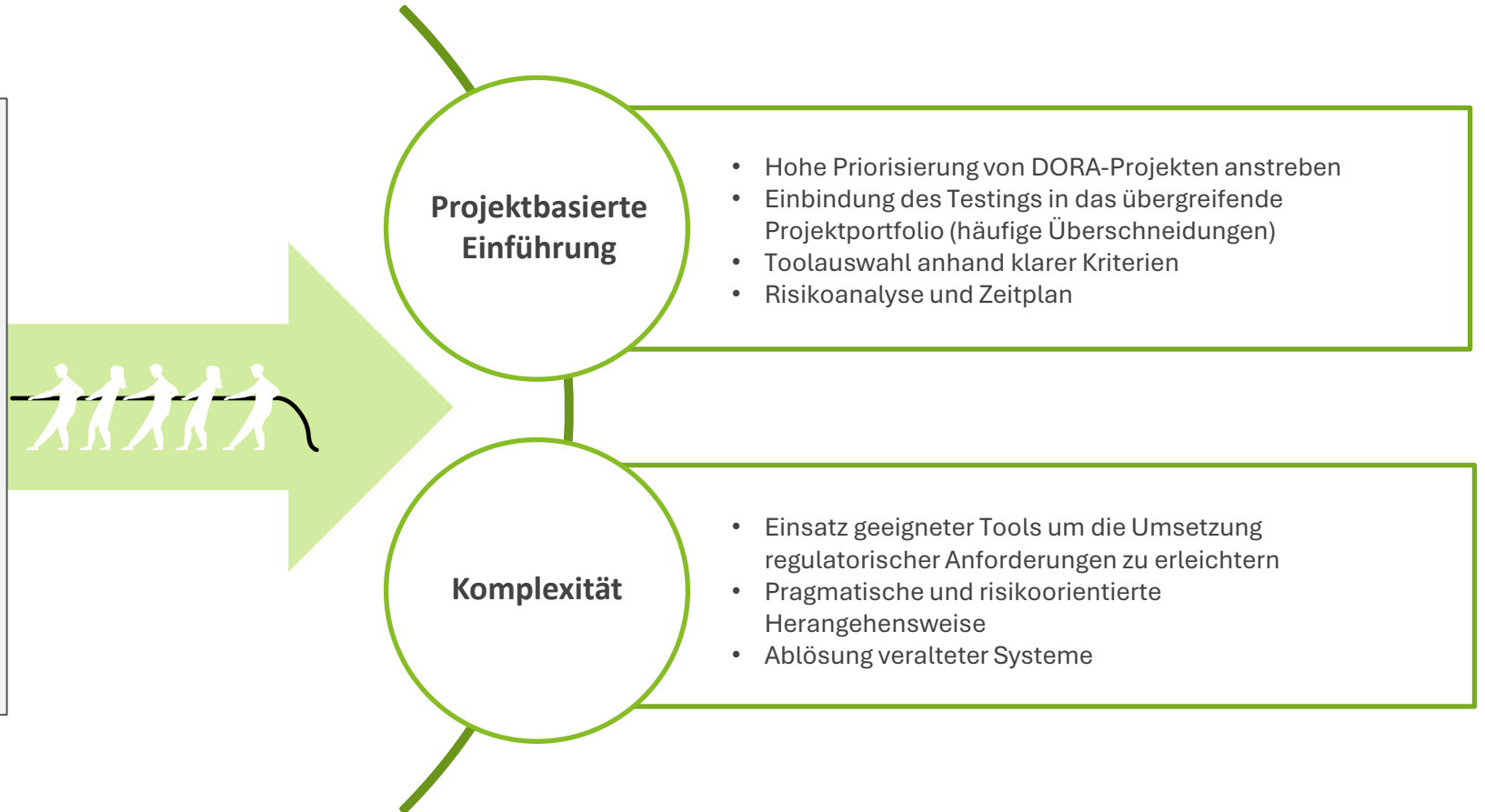
### Herausforderungen

#### Projektbasierte Einführung

- Die Einführung technischer, häufig komplexer, Lösungen erfordert häufig eine eigenständige Projektorganisationen
- Ressourcenkonflikte und weitere Abhängigkeiten mit weiteren laufenden Projekten (Priorisierungsproblem)

#### Komplexität

- Eine Übersicht über verbaute Drittparteienbibliotheken bisher nicht (flächendeckend) am Markt etabliert und (noch) kein einheitlicher Marktstandard vorhanden
- Erschwerte Anbindung veralteter Systeme an neue Testtechnologien
- Erfahrungen mit TLTPs am Markt noch überschaubar



### Erfahrungen & Erkenntnisse

#### Projektbasierte Einführung

- Hohe Priorisierung von DORA-Projekten anstreben
- Einbindung des Testings in das übergreifende Projektportfolio (häufige Überschneidungen)
- Toolauswahl anhand klarer Kriterien
- Risikoanalyse und Zeitplan

#### Komplexität

- Einsatz geeigneter Tools um die Umsetzung regulatorischer Anforderungen zu erleichtern
- Pragmatische und risikoorientierte Herangehensweise
- Ablösung veralteter Systeme

# DORA Kapitel IV Testen der digitalen operationalen Resilienz

## Deep Dive: Open-Source Analyse



Nach Artikel 10, Abs. 2d (DORA, RTS 15 - Risikomanagement) müssen betroffene Finanzunternehmen verwendete **Drittbibliotheken** hinsichtlich potenzieller **Schwachstellen** und **Lizenzierungskonflikten überwachen ('Open-Source Analysen')**. Der Fokus liegt hierbei auf Anwendungen, die **kritische oder wichtige Funktionen unterstützen**, unabhängig davon, ob das Unternehmen über deren Quellcode verfügt.

Die notwendigen Mittel zur Erfüllung der Anforderungen können in unterschiedlichen Formen bereitgestellt werden, z.B.



### Software Bill of Material (SBOM)

- Standardisierte Übersicht über den Aufbau einer Software
- Generierbar in verschiedenen Formaten (z.B. CycloneDX, SPDX)
- Wird von den meisten automatisierten Open-Source Analyse Tools unterstützt



### Liste verwendeter Drittbibliotheken

- Auflistung in Software eingesetzter Drittbibliotheken ohne standardisierte & maschinenlesbare Struktur (z.B. Übermittlung als PDF)
- Manuelle Übertragung in automatisierte Tools erforderlich



### Quellcode

- SBOM kann auf Basis des Quellcodes generiert werden
- Mögliche Aufwände durch Sicherstellung der anforderungs-konformen Verwaltung des Quellcodes von Drittparteien



### Durchführungsnachweis

- Nachweis (z.B. ISAE-Bericht) über die Durchführung von Open-Source Analysen
- Ausweichmöglichkeit, sofern keine der genannten Optionen realisierbar ist
- Regelmäßige Aktualisierung des Nachweises erforderlich

**Deloitte.**

# Management des IKT-Drittparteirisikos Struktur & Herausforderungen

A laptop is open on a dark surface. The screen shows a photograph of several green, leafy plants in black pots, arranged in a row. The text 'Management des IKT-Drittparteirisikos Struktur & Herausforderungen' is overlaid in white on the left side of the screen. The background of the entire image is a blurred indoor garden with various green plants and warm, bokeh-style lights.

# DORA Kapitel V Management des IKT-Drittparteirisikos

## Artikel 28 – Artikel 30

### Artikel 28 (1 - 3)

#### IKT-Drittparteirisikostrategie & Informationsregister

- Verantwortlichkeit der DORA-Compliance verbleibt beim Finanzinstitut
- Entwicklung von Strategien und Leitlinien für das IKT-Drittparteirisiko
- Führung eines Informationsregisters
- Unterrichtung der Behörde über vertr. Vereinbarungen

### Artikel 28 (4 - 5)

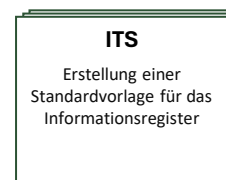
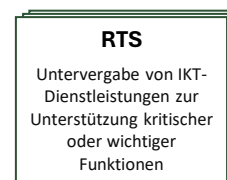
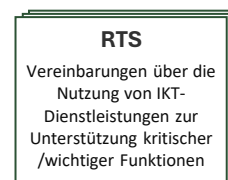
#### Vorvertragliche Bewertung und Informationssicherheit

- Bewertung kritische Funktionen unterstützt werden sollen
- Sicherstellung der Sicherheitsstandards bei IKT-Dienstleistern

### Artikel 28 (6 – 8)

#### Rechte und Ausstiegsstrategien

- Bestimmung der Häufigkeit von Audits und Inspektionen (risikobasiert)
- Vereinbarung von Kündigungsrechten
- Entwicklung von Ausstiegsstrategien sowie die Sicherstellung der Geschäftskontinuität



### Artikel 29

#### Bewertung geplanter vertraglicher Vereinbarungen & Unterauftragsvergabe

- Bewertung der Substituierbarkeit von IKT-Dienstleistern und Prüfung von mehrfachen Verträgen
- Analyse der Risiken der Unterauftragsvergabe von IKT-Dienstleistungen

### Artikel 30 (Abs. 1,2)

#### Schriftliche Verträge und Mindestinhalte

- Schriftliche Dokumentation der Rechte und Pflichten aller Parteien
- Mindestanforderungen an Verträge zu IKT-Dienstleistungen
- Beschreibung der Funktionen und Dienstleistungen, Standorte, Datenschutzbestimmungen, etc.

### Artikel 30 (Abs. 3, 4)

#### Anforderungen für kritische Funktionen und Standardvertragsklauseln

- Zusätzliche Inhalte in Verträgen wie Notfallpläne, Überwachungsrechte, Ausstiegsstrategien
- Nutzung von Standardvertragsklauseln

# DORA Kapitel V Management des IKT-Drittparteirisikos

## Herausforderungen, Erfahrungen und Erkenntnisse

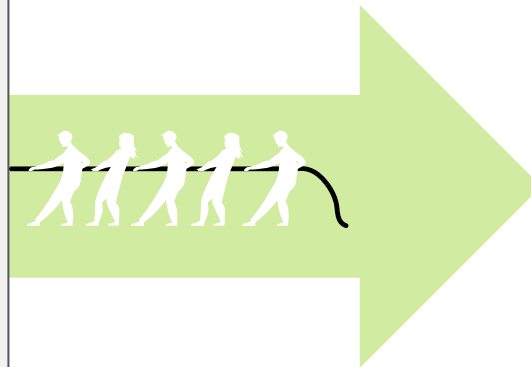
### Herausforderungen

#### Doppelregulierung (MaRisk vs. DORA)

- Umgang mit unterschiedlichen reg. Anforderungen für gleichgelagerte Dienstleistung, bspw. MaRisk und DORA:
  - Auslagerungs- und Informationsregister
  - Exit-Strategien
  - Verträge
  - uvm.

#### Informationsregister

- Datenverfügbarkeit
- Die manuelle Pflege eines Informationsregisters ist ab einer gewissen Größe nicht mehr praktikabel
- Die Entwicklung und die Wartung von Schnittstellen zur Automatisierung ist ressourcenintensiv
- Ggfs. Konsolidierung des Informationsregisters auf Gruppenebene
- Datenvalidierungsregeln der Aufsichtsbehörden nicht harmonisiert



### Erfahrungen & Erkenntnisse

#### MaRisk vs. DORA

- Fokus/Priorisierung auf IKT-Dienstleistungen mit vergleichbaren Steuerungsimpulsen (z.B. kWf & wesentliche Auslagerung)
- Enges Monitoring der aufsichtlichen Verlautbarungen (ins. EBA-GL)

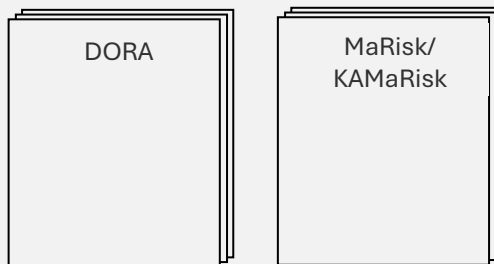
#### Informations- register

- Abwägung in Bezug auf die Automatisierung – Relation zu Anzahl der Dienstleister/Dienstleistungen
- Zentralisierung der Registererstellung und Einreichung (insb. bei Gruppenunternehmen)

# DORA Kapitel V Management des IKT-Drittparteirisikos

## Deep-Dive: Umgang mit der (schrittweisen) Aufhebung der BAIT/KAIT

### Ausgangssituation



Doppelregulierung –  
Beide Anforderungen gelten zur Zeit

#### MaRisk – AT 9 (Auslagerung)


Der isolierte Bezug von Software ist in der Regel als sonstiger Fremdbezug einzustufen. Hierzu gehören u. a. auch die folgenden Unterstützungsleistungen:

- die Anpassung der Software an die Erfordernisse des Kreditinstituts,
- die entwicklungstechnische Umsetzung von Änderungswünschen (Programmierung),
- das Testen, die Freigabe und die Implementierung der Software in die Produktionsprozesse beim erstmaligen Einsatz und bei wesentlichen Veränderungen insbesondere von programmtechnischen Vorgaben,
- Fehlerbehebungen (Wartung) gemäß der Anforderungs-/Fehlerbeschreibung des Auftraggebers oder Herstellers,
- sonstige Unterstützungsleistungen, die über die reine Beratung hinausgehen.

Dies gilt nicht für Software, die zur Identifizierung, Beurteilung, Steuerung, Überwachung und Kommunikation der Risiken eingesetzt wird oder die für die Durchführung von bankgeschäftlichen Aufgaben von wesentlicher Bedeutung ist; bei dieser Software sind Unterstützungsleistungen als Auslagerung einzustufen. Die gleichen Maßstäbe gelten für den Betrieb der Software durch einen externen Dritte

#### KAMaRisk – 10 (Outsourcing)

Eine Auslagerung liegt vor, wenn ein anderes Unternehmen mit der Wahrnehmung von Aufgaben beauftragt wird (Auslagerungsunternehmen), die ansonsten von der Gesellschaft selbst erbracht würden.



Sinngemäße  
Anwendung der KAIT-  
Kriterien

**Deloitte.**

**DORA@Deloitte**



# Ganzheitliche Unterstützung für eine effiziente und sichere DORA-Umsetzung

Durch nationalen und internationalen Austausch gewährleisten wir eine umfassende Expertise für die effiziente Umsetzung der DORA

## Deloitte Banking Union Center (Ebene EMEA)

Über das Deloitte Banking Union Center steuern wir den internationalen Austausch hinsichtlich der neuesten Entwicklung zu DORA.

Hierbei können wir wertvolle Erfahrungen aus den unterschiedlichen DORA-Projekten in ganz Europa austauschen und für einen einheitlichen und umfangreichen Wissensstand sorgen.



## DORA Implementation Board (Deloitte Deutschland)

In Deloitte Deutschland sorgt unser DORA Implementation Board für den aktiven Wissensaustausch und Aufbau.

Die Mitglieder entstammen unseren verschiedenen Service Bereichen wie Audit & Assurance, Deloitte Consulting und Deloitte Legal.

### Ihre Vorteile

- Sie profitieren von dem Know-How unserer europaweiten Deloitte-Experten
- Benchmarking mit nationalen und internationalen Unternehmen
- Zugriff auf die aktuellsten Erkenntnisse und Entwicklungen zu DORA

## DORA Projektteams



## Austausch mit Fachgremien etc.

Unsere Deloitte Mitarbeitenden sind im regelmäßigen Austausch mit den regulierenden Behörden und Aufsichtsorganen.

Wir nehmen an regelmäßigen Sitzungen von Fachgremien (z.B IT-Roundtable Arbeitskreis DORA) teil und gestalten Anwendungs- und Umsetzungshinweise aktiv mit.

## DORA IDW-Arbeitskreis

Wir wirken aktiv an der Erstellung des DORA-Prüfungsstandards und der Arbeitshilfe im Rahmen des IDW PS 528 mit.