BAI – WEBINAR

# DORA – Digitale Resilienz für Investmentfonds & Wertpapierfirmen

**Speaker:**

**Josefine Spengler**, Rechtsanwältin und Fachanwältin für IT-Recht,
Annerton Rechtsanwaltsgesellschaft mbH


**Sina Nennstiel**

Referentin Recht & Policy

Poppelsdorfer Allee 106
53115 Bonn
+49 (0) 228 96987-13
nennstiel@bvai.de


# Speaker

**Josefine Spengler**

- Rechtsanwältin und Fachanwältin für Informationstechnologierecht bei der Annerton Rechtsanwaltsgesellschaft mbH

- Umfassende Beratungstätigkeit zur Umsetzung regulatorischer Anforderungen an IT-Systeme, zu Cybersicherheit und zu Compliance-Fragen

- Autorin von Fachbeiträgen zu aufsichtsrechtlichen IT-Sicherheitsanforderungen

# Agenda

- Eröffnungsworte
- DORA-Anwendungsbereich für AIFs
- Überblick über die wesentlichen Pflichten nach DORA
- Sanktionen bei Nichteinhaltung von DORA
- Quick Wins & Handlungsempfehlungen
- Q & A

# Anstehende Events

## BAI Insight 63

- 8. April 2025 (Köln)

## BAI Alternative Investor Conference

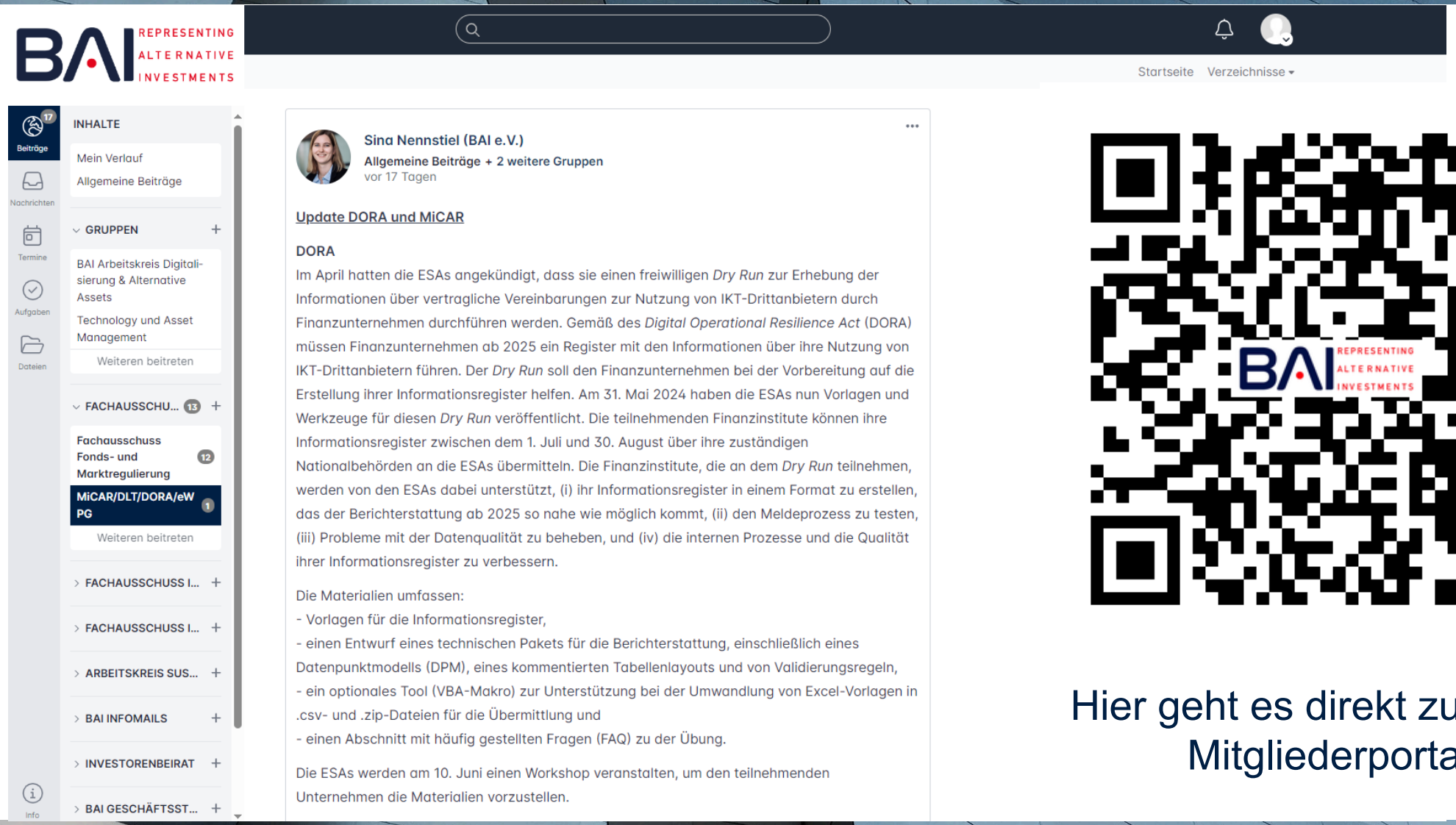
- 7. und 8. Mai 2025
- Pre-Event am 6. Mai 2025

## BAI InnovationsDay

- 30. September 2025 (Berlin)

Hier geht es direkt zum BAI-Eventkalender

# BAI Mitgliederportal: https://www.mitglieder.bvai.de




Hier geht es direkt zum BAI-Mitgliederportal

Treffen des BAI-Arbeitskreises Digitalisierung & Alternative Assets am 31. März 2025 um 16 Uhr, Einwahldaten über das BAI-Mitgliederportal

Hier geht es direkt zum Arbeitskreis auf dem Mitgliederportal

ANNERTON

# Digital Operational Resilience Act

Digitale Resilienz für Investmentfonds & Wertpapierfirmen

BAI Webinar 19.03.2025

ANNERTON

1. DORA - Was ist das?
2. Anwendungsbereich
3. IKT-Risikomanagement
4. IKT-Drittparteien-Management
5. IKT-Vorfallsmanagement
6. DOR–Testing
7. Sanktionen/Nichteinhaltung von DORA
8. Quick Wins/Handlungsempfehlungen

ANNERTON

- DORA (Digital Operational Resilience Act) ist Teil des EU-Pakets zur Digitalisierung des Finanzsektors

- DORA ist am 17.01.2023 in Kraft getreten und findet seit dem 17.01.2025 Anwendung.

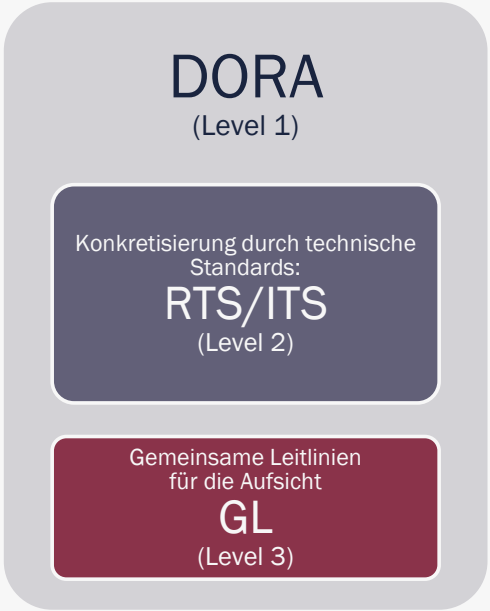

- neuer Fokus der Finanzaufsicht mit DORA:

| | |
|---|---|
| früher: | finanzielle Solidität des Unternehmens |
| mit DORA zusätzlich: | Sicherstellung der Aufrechterhaltung eines widerstandsfähigen Betriebs im Falle einer schwerwiegenden Betriebsunterbrechung |

ANNERTON

# DORA-Level 2 und Level 3 Rechtsakte

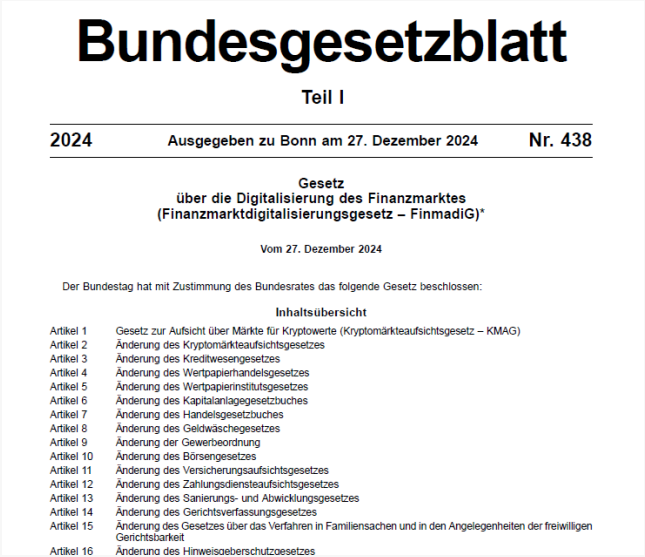
- DORA enthält als Basisrechtsakt **(Level 1)** weitergehende Ermächtigungen für delegierte Rechtsakte und Durchführungsstandards
  - (*Regulatory Technical Standards* – „**RTS**“ und *Implementing Technical Standards* – „**ITS**“) **(Level 2)**
  - gemeinsame Leitlinien („**GL**“) **(Level 3)**



ANNERTON

# DORA - Umsetzung in Deutschland

- Umsetzung DORA in Deutschland über das „Gesetz über die Digitalisierung des Finanzmarktes“ (FinmadiG) mit weitreichenden Änderungen z.B. im KWG und KAGB
- Am **27.12.2024** im Bundesgesetzblatt veröffentlicht und zwischenzeitlich in Kraft getreten.
- weitreichenden Änderungen der nationalen Gesetze im Bereich Finanzaufsicht, z.B. im KWG und KAGB
- Über die Implementierungen in die nationalen Gesetze durch das FinmadiG wird die Prüfung der DORA-Anforderungen durch den Jahresabschlussprüfer verbindliche Vorgabe



**Bundesgesetzblatt**

**Teil I**

**2024** **Ausgegeben zu Bonn am 27. Dezember 2024** **Nr. 438**

**Gesetz**
**über die Digitalisierung des Finanzmarktes**
**(Finanzmarktdigitalisierungsgesetz – FinmadiG)***

**Vom 27. Dezember 2024**

Der Bundestag hat mit Zustimmung des Bundesrates das folgende Gesetz beschlossen:

**Inhaltsübersicht**

ANNERTON

# DORA - Umsetzung in Deutschland

Mit dem Wirksamwerden von DORA hat die BaFin folgende aufsichtliche Anforderungen an die IT zum 17.01.2025 aufgehoben:

- **KAIT:** Kapitalverwaltungsaufsichtliche Anforderungen an die IT (Rundschreiben 11/2019 (WA) in der Fassung vom 01.10.2019)
- **VAIT:** Versicherungsaufsichtliche Anforderungen an die IT (Rundschreiben 10/2018 in der Fassung vom 03.03.2022)
- **ZAIT:** Zahlungsdiensteaufsichtliche Anforderungen an die IT von Zahlungs- und E-Geld-Instituten (Rundschreiben 11/2021 (BA) in der Fassung vom 16.08.2021)

Die folgenden aufsichtliche Anforderungen an die IT gibt es noch bis 31.12.2026. Sie gelten aber nicht mehr für Institute, die seit 17.01.2025 den DORA anwenden:

- **BAIT:** Bankaufsichtliche Anforderungen an die IT (Rundschreiben 10/2017 (BA) in der Fassung vom 16.12.2024)

ANNERTON

# Ziele von DORA

**Harmonisierung**
der aufsichtsrechtlichen Anforderungen durch ein einheitliches Regelwerk

**Rechtssicherheit**
insbesondere für grenzüberschreitend tätige Finanzunternehmen

**Vereinfachungen**
insbesondere im Meldewesen
(vgl. Cyberbedrohungen, zahlungsbezogene Sicherheitsvorfälle)

**Stabilität**
und Integrität der Finanzmärkte erhalten

**Verbraucherschutz**
durch ein hohes IT-Sicherheitsniveau

ANNERTON

# DORA - Geltungsbereich

Gemäß Art. 2 (1) DORA umfasst der Anwendungsbereich alle in Europa beaufsichtigten Finanzunternehmen, u.A.:

Kreditinstitute;
Zahlungsinstitute;
Kontoinformationsdienste;
E-Geld-Institute;
Investmentfirmen;
Wertpapierfirmen

Anbieter von Krypto-Dienstleistungen

Verwaltungsgesellschaften;
Verwalter alternativer Investmentfonds;
Versicherungs- und Rückversicherungsunternehmen;
Versicherungsvermittler;
Zentralverwahrer;
Zentrale Gegenparteien

Schwarmfinanzierungs-dienstleister;
Ratingagenturen;
Handelsplätze;
Transaktionsregister;
Ratingagenturen;
Einrichtungen d. betrieblichen Altersversorgung

**IKT-Drittdienstleister** (inkl. gruppeninterne IKT-Dienstleister)

ANNERTON

Art. 2 Abs. 1 lit. e) DORA

# DORA - Geltungsbereich

## Wertpapierfirmen

- im Sinne von Artikel 4 Absatz 1 Nummer 1 der Richtlinie 2014/65/EU (MiFID II)= *„jede juristische Person, die im Rahmen ihrer üblichen beruflichen oder gewerblichen Tätigkeit gewerbsmäßig eine oder mehrere Wertpapierdienstleistungen für Dritte erbringt und/oder eine oder mehrere Anlagetätigkeiten ausübt.“ (...)*

- Ausgenommen sind gemäß Art. 2 Abs. 3 lit d) DORA : => gemäß den Artikeln 2 und 3 der Richtlinie 2014/65/EU (MiFID II) ausgenommene natürliche oder juristische Personen = natürliche und juristische Personen, die Wertpapierdienstleistungen erbringen dürfen, ohne eine Zulassung gemäß MiFID II oder aufgrund nationalen Rechts erhalten zu müssen.

= Zulassungspflichtige Wertpapierfirmen

ANNERTON

Art. 2 Abs. 1 lit. l) DORA

# DORA - Geltungsbereich

## Verwaltungsgesellschaften

- im Sinne von Artikel 2 Abs. 1 lit. b der Richtlinie 2009/65/EG (OGAW-RiLi/UCITS-Directive)= *„Gesellschaft, deren reguläre Geschäftstätigkeit in der Verwaltung von in der Form eines Investmentfonds oder einer Investmentgesellschaft konstituierten Organismen für gemeinsame Anlagen in Wertpapieren (OGAW) besteht (gemeinsame Portfolioverwaltung).“*

  = erlaubnispflichtige KVGen (KAGB-Institute)

OAGW: Organismus für gemeinsame Anlagen in Wertpapieren
UCITS: Undertakings for Collective Investments in Transferable Securities

ANNERTON

Art. 2 Abs. 1 lit. k) DORA

# DORA - Geltungsbereich

## Verwalter alternativer Investmentfonds

- im Sinne von Artikel 4 Abs. 1 lit. b der RL 2011/61/EU (AIFMD) = *„jede juristische Person, deren reguläre Geschäftstätigkeit darin besteht, einen oder mehrere AIF zu verwalten.“*

- Ausgenommen sind gemäß Art. 2 Abs. 3 lit a) DORA: => Verwalter alternativer Investmentfonds im Sinne von Artikel 3 Absatz 2 AIFMD: (registrierte KVGen)
  - a) AIFM, die entweder direkt oder indirekt über eine Gesellschaft, mit der der AIFM über eine gemeinsame Geschäftsführung, ein gemeinsames Kontrollverhältnis oder durch eine wesentliche direkte oder indirekte Beteiligung verbunden ist, die Portfolios von AIF verwalten, deren verwaltete Vermögenswerte — einschließlich der durch Einsatz von Hebelfinanzierungen erworbenen Vermögenswerte — insgesamt nicht über einen Schwellenwert von 100 Mio. EUR hinausgehen, oder
  - b) AIFM, die entweder direkt oder indirekt über eine Gesellschaft, mit der sie über eine gemeinsame Geschäftsführung, ein gemeinsames Kontrollverhältnis oder durch eine wesentliche direkte oder indirekte Beteiligung verbunden sind, die Portfolios von AIF verwalten, deren verwaltete Vermögenswerte insgesamt nicht über einen Schwellenwert von 500 Mio. EUR hinausgehen, wenn die Portfolios dieser AIF aus nicht hebelfinanzierten AIF bestehen, die für einen Zeitraum von fünf Jahren nach der Tätigung der ersten Anlage in jeden dieser AIF keine Rücknahmerechte ausüben dürfen.

= (registrierte KVGen)

➢ Berechnung der Schwellenwerte unterliegt komplexen Anforderungen - ob die genannten Schwellenwerte erreicht werden oder nicht, ist letztendlich eine Einzelfallbetrachtung durch die Aufsicht (siehe hierzu auch ESMA Q&A 697 v. 10.03.2023: *„The notion of “substantive direct or indirect holding” shall be assessed on a case-by-case basis by AIFMs supervisors.”*)

ANNERTON

§ 1a Abs. 2 KWG

# DORA - Geltungsbereich

## weitere KWG-Institute (>> FinmadiG):

Institute, die unter das KWG fallen, jedoch nicht ausdrücklich als „Finanzunternehmen“ in DORA genannt sind, müssen gemäß § 1a Abs. 2 KWG ebenfalls DORA erfüllen wie ein CRR-Institut. Allerdings findet nur ein erleichterter DORA-Rahmen Anwendung:

- vereinfachter IKT-Risikomanagement-Rahmen im Sinne von Art. 16 DORA
- keine Pflicht zum DOR-Testing im Sinne der Art. 26/27 DORA
- keine Anwendung der Vorgaben zum IKT-Drittparteienmanagement im Sinne der Art. 28-30 DORA

erst ab 01.01. 2027

§ 1a Abs. 2a KWG findet erst ab dem 01.01.2027 Anwendung. Die Anforderungen zum Meldewesen bei **IKT-Vorfall** müssen jedoch bereits ab dem 17.01.2025 angewendet werden (vgl. § 65a KWG – Übergangsvorschrift zum FinmadiG). Für die betroffenen Institute gilt bis zum 31.12.2026 ansonsten noch die BAIT.

*Beispiele: Finanzierungsleasing und Factoring*

ANNERTON

Art. 16 DORA

# DORA – Erleichterungen innerhalb von DORA

## Vereinfachter IKT-Risikomanagement-Rahmen findet Anwendung auf:

- KWG-Institute, die keine Finanzunternehmen im Sinne von DORA sind (§ 1a Abs.2 KWG – ab 01.01.2027)

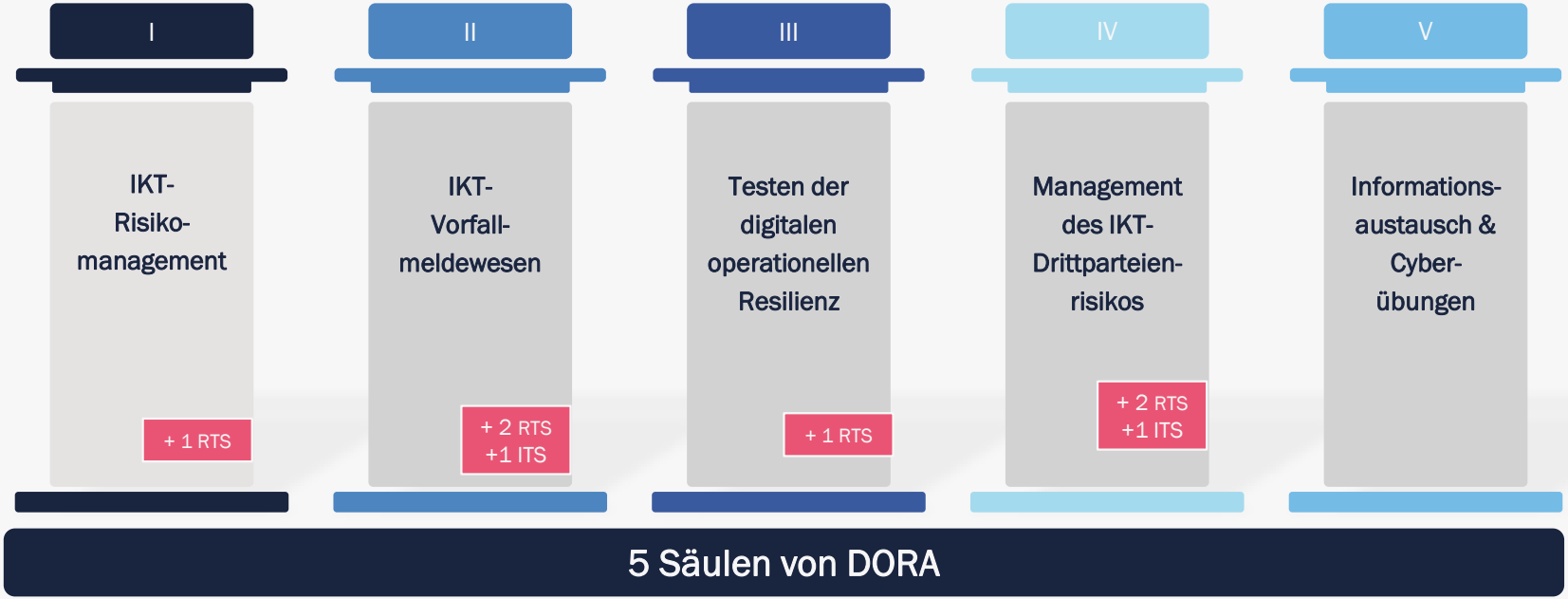
- kleine und nicht verflochtene **Wertpapierfirmen** (Art. 16 Abs. 1 DORA)
  kleine Wertpapierinstitute nach dem Wertpapierinstitutsgesetz

- **Kleinstunternehmen**
  (Art. 3 Nr. 60 DORA = Finanzunternehmen, das weniger als zehn Personen beschäftigt und dessen Jahresumsatz bzw. -bilanzsumme 2 Mio. EUR nicht überschreitet.)

Der vereinfachte Rahmen für das IKT-Risikomanagement besteht aus den gleichen wesentlichen Grundbausteinen wie der allgemeine IKT-Risikomanagement-Rahmen, bietet jedoch ein höheres Maß an Flexibilität durch weniger spezifische Anforderungen und nimmt einige Anforderungen ganz aus. Er wird durch einen technische Regulierungsstandard (RTS) weiter konkretisiert.

ANNERTON

# DORA – Aufbau und Inhalte




*IKT = Informations- und Kommunikationstechnologie

ANNERTON

Kap. II,
Art. 5-16 DORA

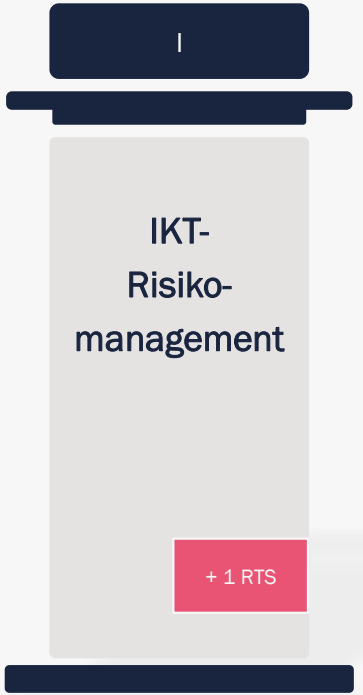
# IKT-Risikomanagement

- Finanzunternehmen sollen über einen
  - soliden,
  - umfassenden und
  - gut dokumentierten

  Rahmen für das IKT-Risikomanagement verfügen.

- Ziel: IKT-Risiken schnell, effizient und umfassend angehen und hohes Maß an digitaler operativer Widerstandsfähigkeit gewährleisten

- Umsetzungsaufwand:  HOCH



ANNERTON

Art. 6 (3) DORA

# IKT-Risikomanagementrahmen

- Finanzunternehmen sind verpflichtet, ein **umfassendes IKT-Risikomanagement** einzurichten, dazu gehört:
  - Vorhalten einer Digital Operational Resilience (DOR-) Strategie
  - Einrichtung und Pflege belastbarer IKT-Systeme und -Werkzeuge, die die Auswirkungen von IKT-R minimieren,
  - Identifizierung, Klassifizierung und Dokumentation kritischer IKT-Funktionen,
  - kontinuierliche Überwachung aller Quellen von IKT-Risiken
  - sofortige Erkennung von anomalen Aktivitäten,
  - Einführung spezieller und umfassender Business-Continuity-Richtlinien sowie Notfall- und Wiederherstellungspläne, einschließlich jährlicher Tests der Pläne
  - Einrichtung von Mechanismen, um sowohl aus externen Ereignissen als auch aus eigenen IKT-Vorfällen zu lernen und sich weiterzuentwickeln.

ANNERTON

Kap. II,
Art. 5-16 DORA

# IKT-Risikomanagement

- **Leitungsorgan wird mit DORA persönlich** stärker verpflichtet

- **Verantwortungen des Leitungsorgans** nach DORA:

  - Gesamtverantwortung für die Festlegung und Genehmigung der Strategie für die digitale operationale Resilienz liegt beim Management

  - Letztverantwortung für IKT-Risiken des Finanzunternehmens liegt beim Management

  - Verpflichtung für das Management, angemessene Budgetmittel für den IKT-Risikomanagementrahmen bereit zu stellen

  - Mitglieder des Leitungsorgans müssen ausreichende Kenntnisse und Fähigkeiten im Bereich IT-Sicherheit haben und auf dem neuesten Stand halten, um ihre Aufgaben adäquat wahrnehmen zu können
    (=> jährliche Management-Schulungen zu IKT-Risikomanagement notwendig)

BOARD OF DIRECTORS

ANNERTON

Art. 7 DORA

# IKT-Risikomanagement

- Art. 7 DORA:

- IKT-Systeme, -Protokolle und –Tools von Finanzunternehmen müssen

  - stets auf dem neuesten Stand gehalten,
  - angemessen,
  - zuverlässig,
  - mit ausreichenden Kapazitäten (finanziell und personell) ausgestattet und
  - technologisch resilient

  sein.

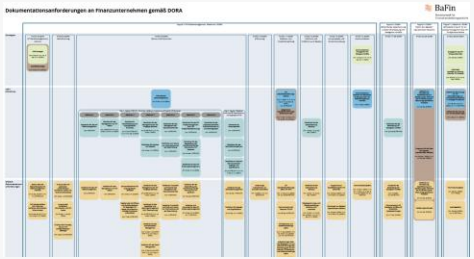
ANNERTON

Art. 6 (5) DORA

# IKT-Risikomanagement

- IKT-Risikomanagement-Rahmen :

- DORA-RTS zum Risikomanagementrahmen gibt inhaltliche Vorgaben zu mehr als 20 Themenkomplexen, z.B. für:
  - Management von IKT-Assets
  - Verschlüsselung und kryptografische Kontrollen
  - Management von IKT-Vorgängen (inkl. Kontrollen und Überwachung für IKT-Systeme)
  - Kapazitäts- und Leistungsmanagement
  - Schwachstellen- und Patch-Management
  - Logging
  - Daten- und Systemsicherheit
  - Management der Netzwerksicherheit
  - IKT-Projektmanagement
  - IKT Change Management
  - Personalpolitik
  - Identitätsmanagement
  - Zugangskontrolle
  - IKT-Vorfallsmanagement
  - Geschäftsfortführung im Krisenfall



- IKT-Risikomanagement-Rahmen ist regelmäßig zu überprüfen und inkl. Dokumentation zu aktualisieren:
  - mindestens 1x jährlich* oder
  - nach schwerwiegenden Vorfällen oder
  - nach aufsichtsrechtlicher Anweisung oder
  - nach Feststellungen im Audit
  - nach Feststellungen durch Tests

*bei Kleinstunternehmen: regelmäßig

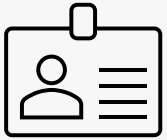
Siehe dazu auch: BaFin Dokumentationsanforderungen nach DORA unter
https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2024/meldung_2024_12_17_Dokumentationsanforderungen_DORA.html

ANNERTON

Art. 6 (4)
DORA

# IKT-Risikomanagement

- Neue Funktion:
  IKT-Risikomanager



- Art. 6 (4) DORA:
  *Finanzunternehmen übertragen die Zuständigkeit für das Management und die Überwachung des IKT-Risikos an eine Kontrollfunktion und stellen ein angemessenes Maß an Unabhängigkeit dieser Kontrollfunktion sicher, um Interessenkonflikte zu vermeiden.*

- *Die Finanzunternehmen sorgen für eine angemessene Trennung und Unabhängigkeit von IKT-Risikomanagementfunktion, Kontrollfunktionen und internen Revisionsfunktionen gemäß dem Modell der drei Verteidigungslinien oder einem internen Modell für Risikomanagement und Kontrolle.*

Aufgaben IKT-Risikomanager:

ANNERTON

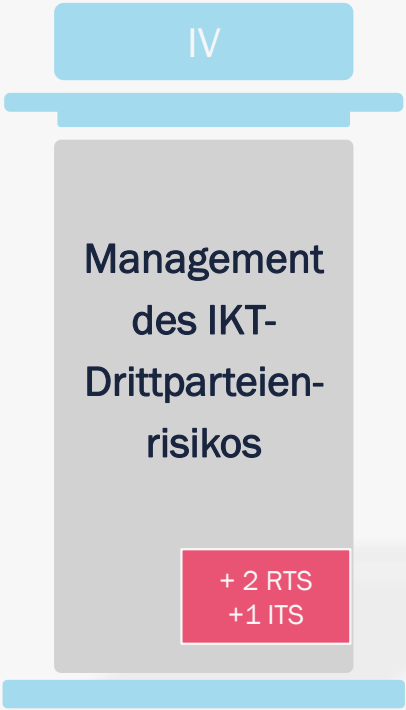
Kap. V,
Art. 28-30 DORA

# Management von IKT-Drittparteienrisiken

- solide Überwachung des IKT-Drittparteienrisikos erforderlich

- Mindestaspekte für eine vollständige Überwachung des IKT-Drittparteienrisikos durch das Finanzinstitut entlang des gesamten Lebenszyklus von Auslagerungen bzw. sonstiger Fremdbezüge von IT-Dienstleistungen

- Umsetzungsaufwand:  HOCH



ANNERTON

Kap. V,
Art. 28-30 DORA

# Management von IKT-Drittparteienrisiken

**IKT-Dienstleister Begriff**

- Art. 3 Nr.19 DORA:
  *„IKT-Dienstleister ist ein Unternehmen, das IKT-Dienstleistungen anbietet.“*

- Art. 3 Nr. 21 DORA:
  *„IKT-Dienstleistungen“ sind: 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*

- In Annex III des DORA-ITS zum IKT-Auslagerungsregister ist eine (wohl abschließende) Auflistung der IKT-Dienstleister erhalten. Danach sind folgende Dienstleistungen von der DORA erfasst:

| 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 | |

ANNERTON

Kap. V,
Art. 28-30 DORA

# Management von IKT-Drittparteienrisiken

**Neue Auslagerungsmatrix**

DORA kennt den Begriff „Auslagerung“ nicht, DORA unterscheidet bei IKT-Bezug stattdessen zwischen:

- **„kritische oder wichtige Funktion“**
  eine Funktion, deren Ausfall die finanzielle Leistungsfähigkeit eines Finanzunternehmens oder die Solidität oder Fortführung seiner Geschäftstätigkeiten und Dienstleistungen erheblich beeinträchtigen würde oder deren unterbrochene, fehlerhafte oder unterbliebene Leistung die fortdauernde Einhaltung der Zulassungsbedingungen und -verpflichtungen eines Finanzunternehmens oder seiner sonstigen Verpflichtungen nach dem anwendbaren Finanzdienstleistungsrecht erheblich beeinträchtigen würde (Art. 3 Nr. 22 DORA)

- **nicht-kritische/nicht-wichtige Funktion**

ANNERTON

Kap. V,
Art. 28-30 DORA

# Management von IKT-Drittparteienrisiken

IKT-Dienstleister Begriff

- **Folge:**
  - auch IKT-Bezug, der bisher nicht unter den Auslagerungsbegriff viel, kann nun unter den Anwendungsbereich der DORA fallen (z.B.: IKT-Beratung/Einsatz von externen Programmierern)
  - auch der Bezug von nicht-kritischen/nicht-wichtigen IKT-Funktionen fällt unter den Anwendungsbereich von DORA
  - **Dies führt dazu, dass jeder IKT-Drittbezug überprüft und im Sinne von DORA neu eingestuft werden muss !**

ANNERTON

Art. 30
DORA

# Management von IKT-Drittparteienrisiken

**Verträge mit IKT-Drittdienstleistern**

- Vertragliche Vereinbarungen mit IKT-Drittanbietern müssen bestimmte Mindestanforderungen an Regelungsgehalt und -tiefe erfüllen (vgl. Art. 30 Abs. 2 DORA), u.A.:
  - klare und vollständige **Beschreibung aller Funktionen** und IT-Dienstleistungen;
  - ob und unter welchen Bedingungen **Sub-Auslagerung** für eine IT-Dienstleistung, die eine kritische oder wichtige Funktion unterstützt, zulässig ist;
  - Bestimmungen über **Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit** in Bezug auf den Schutz von **Daten**, einschließlich personenbezogener Daten;
  - die Verpflichtung des IKT-Drittdienstleisters, dem Finanzunternehmens im Falle eines **IKT-Vorfalls** ohne zusätzliche Kosten oder zu im Voraus festgelegten Kosten Unterstützung zu leisten;
  - besondere **Kündigungsrechte** und entsprechende Mindestkündigungsfristen für die Beendigung des Vertragsverhältnisses (vgl. Art. 28 Abs. 7 DORA)

ANNERTON

Art. 30
DORA

# Management von IKT-Drittparteienrisiken

**Verträge mit IKT-Drittdienstleistern**

- Eine vertragliche Vereinbarung über die Nutzung von IKT-Diensten, die kritische oder wichtige Funktionen unterstützen, muss zusätzlich u.A. Folgendes enthalten (vgl. Art. 30 Abs. 3 DORA), u.A.:

  - **vollständige Leistungsbeschreibungen (SLAs)**, einschließlich genauer quantitativer und qualitativer Leistungszielen (KPIs)
  - besondere **Berichtspflichten**
  - das Recht zu uneingeschränkten **Inspektionen** und **Audits**
  - Anforderungen an den IKT-Drittdienstleister, **Notfallpläne** zu implementieren und zu testen
  - **Ausstiegsstrategien**, insbesondere die Festlegung eines verbindlichen angemessenen Übergangszeitraums

ANNERTON

Art. 30
DORA

# Management von IKT-Drittparteienrisiken

## Verträge mit IKT-Drittdienstleistern

- **Achtung:**

  Die vertraglichen Anforderungen aus Art. 30 DORA gelten auch für bestehende Verträge, die vor Inkrafttreten der DORA abgeschlossen wurden.

  ↓

  Bestehende Verträge müssen deshalb gemäß den Anforderungen von DORA neu verhandelt und durch entsprechende Änderungsverträge mit den Anforderungen von DORA in Einklang gebracht werden.

ANNERTON

Art. 28
DORA

# Management von IKT-Drittparteienrisiken

**Dokumentation des IKT-Drittparteienrisikos**

- Art. 28 Abs. 2 - 3 DORA stellt **allgemeine Anforderungen an das Management des IKT-Drittparteienrisikos:**
  - Verabschiedung und regelmäßige Überprüfung einer Strategie zum IKT-Drittparteienrisiko (>>> Auslagerungs-Richtlinie!)
  - Festlegung einer eigenen Leitlinie für die Nutzung von IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen (kann in die Auslagerungs-Richtlinie integriert werden)
  - Führen und Aktualisieren eines Informationsregisters in Bezug auf alle vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen

    (Frist zur erstmaligen Einreichung des DORA-Informationsregisters bei der BaFin (über MVP-Portal, Fachverfahren DORA) endet am **11.04.2025** !)
- Art. 28 Abs. 4 - 8 DORA geben Due Diligence-Anforderungen, die vor dem Vertragsabschluss mit einem IKT-Drittdienstleister erfüllt sein müssen (Bewertung des Dienstleisters und Auslagerungsrisikoanalyse)

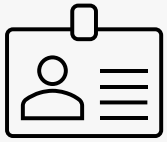
ANNERTON

Art. 14 (3) DORA

# Management von IKT-Drittparteienrisiken

**Neue Funktion:**

- Neue Funktion: IKT-Auslagerungsmanager



- Art. 5 (3) DORA:

*„Finanzunternehmen, bei denen es sich nicht um Kleinstunternehmen handelt, richten eine Funktion ein, um die mit IKT-Drittdienstleistern über die Nutzung von IKT-Dienstleistungen geschlossenen Vereinbarungen zu überwachen, oder benennen ein Mitglied der Geschäftsleitung, das für die Überwachung der damit verbundenen Risikoexposition und die einschlägige Dokumentation verantwortlich ist.“*

- Funktion vergleichbar mit der Funktion des (zentralen) Auslagerungsbeauftragten (Personenidentität ist möglich)

Aufgaben IKT-Auslagerungsmanager:

ANNERTON

# IKT-Vorfälle

Kap. III,
Art. 17-23 DORA

II

IKT-
Vorfall-
meldewesen

+ 2 RTS
+1 ITS

- Verpflichtung, einen Managementprozess zu implementieren, der neben der Behandlung von IKT-bezogenen Vorfällen auch die Überwachung, Protokollierung und Meldung von IKT-bezogenen Vorfällen umfasst.

- Schwerwiegende IKT-Vorfälle müssen unter Verwendung einer Vorlage an die zuständigen Behörden gemeldet werden. Dafür müssen sie nach festgelegten Kriterien klassifiziert werden, um eine Harmonisierung der Meldungen zu erreichen.

- Umsetzungsaufwand:  MITTEL

ANNERTON

# IKT-Vorfälle

Kap. III,
Art. 17-23 DORA

Definition IKT-Vorfall:

- Art. 3 Nr. 8 DORA - „IKT-bezogener Vorfall“ :
  *ein von dem Finanzunternehmen nicht geplantes Ereignis bzw. eine entsprechende Reihe verbundener Ereignisse, das bzw. die die **Sicherheit der Netzwerk- und Informationssysteme beeinträchtigt** und **nachteilige Auswirkungen** auf die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von **Daten oder** auf die vom Finanzunternehmen erbrachten **Dienstleistungen** hat;*

- Art. 3 Nr. 9 DORA „zahlungsbezogener Betriebs- oder Sicherheitsvorfall“.
  *ein von Finanzunternehmen nicht geplantes Ereignis bzw. eine entsprechende Reihe verbundener Ereignisse, unabhängig davon, ob es sich um IKT-bezogene Vorfälle handelt oder nicht, das bzw. die nachteilige Auswirkungen auf die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit **zahlungsbezogener Daten** oder auf die vom Finanzunternehmen bereitgestellten **zahlungsbezogenen Dienste** hat;*

- Art. 3 Nr. 10 DORA – „schwerwiegender IKT-bezogener Vorfall“:
  *ein IKT-Vorfall, der umfassende nachteilige Auswirkungen auf die Netzwerk- und Informationssysteme hat, die **kritische oder wichtige Funktionen** des Finanzunternehmens unterstützen;*

Kritische/wichtige Funktionen: diejenigen Aktivitäten und Prozesse, deren Beeinträchtigung eine erhebliche Beeinträchtigung der finanziellen Leistungsfähigkeit oder der Geschäftsfortführung zur Folge hätte.

ANNERTON

Art. 19 Abs. 1 DORA

# IKT-Vorfälle

- Sämtliche Vorfälle müssen von Finanzunternehmen gemäß den in Art. 18 DORA genannten Kriterien klassifiziert und dokumentiert werden.

- schwerwiegende Vorfälle müssen an die Aufsicht gemeldet werden.

- Ein Vorfall wird als schwerwiegender Vorfall angesehen, wenn **kritische** Dienste beeinträchtigt und eine der folgenden beiden Bedingungen erfüllt ist:

  a) Die Wesentlichkeitsschwelle „erfolgreicher böswilliger und unbefugter Zugriff auf Netzwerk- und Informationssysteme, sofern dieser Zugriff zu Verlusten von Daten führen kann“ ist erreicht;

  b) zwei oder mehr der anderen Wesentlichkeitsschwellen sind erreicht

  Achtung: Auch wiederholte Fälle sind in ihrer Gesamtheit zu berücksichtigen, wenn sie innerhalb der letzten 6 Monate mind. 2x aufgrund derselben Fehlerquelle auftreten und zusammengenommen die Schwellenwerte erreichen.

ANNERTON

Art. 6
RTS/ITS Meldung

# IKT-Vorfälle

**Meldefristen bei IKT-bezogenen Vorfällen**

- folgende Fristen zur Abgabe von Meldungen sind strikt einzuhalten:

| Frist | Meldung |
|---|---|
| < 4 h nach Klassifizierung als schwerwiegend | Abgabe einer Erstmeldung |
| < 24 h nach Kenntnis von Vorfall | Abgabe einer Erstmeldung |
| spätestens 72 h nach Erstmeldung + nach Wiederaufnahme Geschäftsbetrieb | Zwischenmeldung spätestens 72 Stunden nach Übermittlung der Erstmeldung, auch wenn sich der Status oder die Handhabung des Vorfalls nicht geändert hat. Die Finanzunternehmen übermitteln unverzüglich etwaige aktualisierte Zwischenmeldungen, in jedem Fall aber, sobald der reguläre Geschäftsbetrieb wiederaufgenommen wurde. |
| < 1 Monat nach Vorlage des letzten aktualisierten Zwischenberichts | Vorlage eines Abschlussberichtes, der Informationen zur Ursache des Vorfalls und zu den Maßnahmen enthält, die ergriffen wurden, um ihn zu beheben und ein erneutes Auftreten zu verhindern. |

ANNERTON

Art. 17 Abs. 2 DORA

# IKT-Vorfälle

**IKT-Vorfall Management durch:**

- Einsatz von Frühwarnindikatoren und Tools zur Früherkennung von Vorfällen
- Verfahren für Reaktionsmaßnahmen bei IKT-bezogenen Vorfällen, um Auswirkungen zu mindern und sicherzustellen, dass die Dienste zeitnah verfügbar und sicher werden.
- Verfahren zur Ermittlung, Nachverfolgung, Protokollierung, Kategorisierung und Klassifizierung IKT-bezogener Vorfälle entsprechend ihrer Priorität und Schwere und entsprechend der Kritikalität der betroffenen Dienste (ICT incident reporting procedure)
- klare Zuweisung von Funktionen und Zuständigkeiten, die bei verschiedenen Arten von IKT-bezogenen Vorfällen und -Szenarien aktiviert werden müssen
- Vorhalten von Kommunikationsplänen für die Kommunikation mit Personal, externen Interessenträgern und Medien sowie für die Benachrichtigung von Kunden, für interne Eskalationsverfahren, einschließlich IKT-bezogener Kundenbeschwerden, und für die Bereitstellung von Informationen an andere Finanzunternehmen, die als Gegenparteien fungieren, ausgearbeitet, je nach Sachlage;
- Sicherstellung, dass zumindest schwerwiegende IKT-bezogene Vorfälle der zuständigen höheren Führungsebene gemeldet werden und die Geschäftsleitung informiert wird, wobei die Auswirkungen und Gegenmaßnahmen und zusätzliche Kontrollen erläutert werden, die infolge dieser IKT-bezogenen Vorfälle einzurichten sind;

ANNERTON

Art. 14 (3) DORA

# IKT-Vorfälle

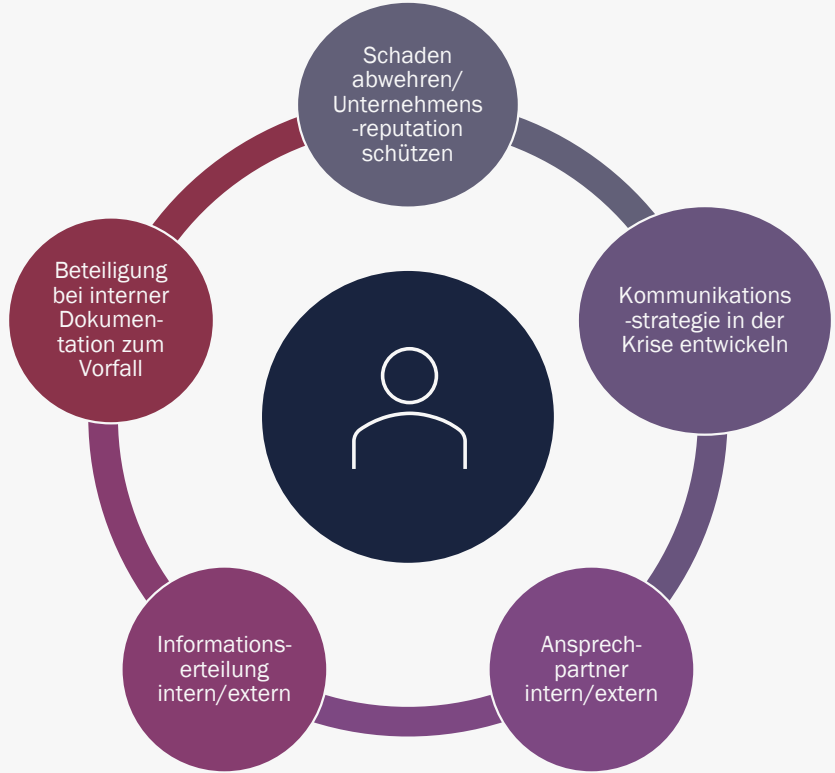
**IKT-Vorfall Management – interne Umsetzung**

- Neue Funktion: Krisenkommunikations-Manager

- Art. 14 (3) DORA:

  *„Mindestens eine Person im Finanzunternehmen ist mit der Umsetzung der Kommunikationsstrategie für IKT-bezogene Vorfälle beauftragt und nimmt zu diesem Zweck die entsprechende Aufgabe gegenüber der Öffentlichkeit und den Medien wahr.“*

Aufgaben Krisenkommunikations-Manager:



ANNERTON

Kap. IV,
Art. 24 - 27 DORA

# Resilienz (DOR) -Testing

- DORA verpflichtet alle Finanzunternehmen dazu, ihre Informations- und Kommunikationstechnologie auf Herz und Nieren zu prüfen, indem sie ein risikobasiertes, proportionales Testprogramm etablieren sollen.
- Die Erstellung dieses Programms liegt in der Verantwortung der einzelnen Finanzinstitute, da es an die Besonderheiten jedes einzelnen angepasst werden muss.
- BaFin versteht **Testen** als ein Instrument für Finanzunternehmen (und die Aufsicht) zu **überprüfen, ob das Ziel der digitalen operationalen Resilienz erreicht wird**
- Umsetzungsaufwand:  MITTEL

III

Testen der digitalen operationellen Resilienz

+ 1 RTS

ANNERTON

Kap. IV,
Art. 24 - 27 DORA

# Resilienz-Testing

- Finanzunternehmen haben ein Programm für Tests der digitalen operationalen Resilienz zu etablieren und zu pflegen.

- Dies beinhaltet:

  - **grundlegende Basis/Standard-Tests** von Schwachstellenbewertung und –scans bis Penetrationstests für alle Finanzunternehmen (Art. 25 DORA)

  - **erweiterte Tests** wie Threat-Led Penetration-Tests (bedrohungsorientierte Penetrationstests, „TLPT“) - nur für Finanzunternehmen, die aus IKT-Perspektive ausgereift genug und von gewisser systemischer Relevanz sind (Art. 26 DORA)

    - Die BaFin informiert betroffene Finanzunternehmen über ihre Verpflichtung zu TLPT.
    - bisher keine Kenntnis über Zeitpunkt der Information
    - Nach Information zur Verpflichtung zu TLPT: 3 Jahre Umsetzungszeit

ANNERTON

Kap. IV,
Art. 24 - 27 DORA

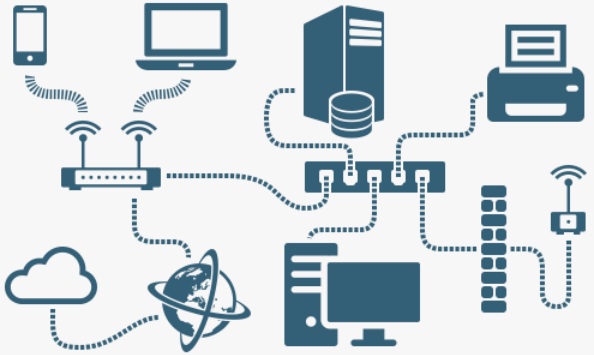
# Resilienz-Testing

Da das Testprogramm **integraler Bestandteil** des IKT-Risikomanagementrahmens (Art. 6 (5) DORA) ist, umfassen die Tests

- alle IKT- und Informationswerte, d. h. Software, Hardware oder Server, aber auch Daten, die eigenständige Werte darstellen.

- alle physischen Komponenten und Infrastrukturen, die für den Schutz von Vermögenswerten relevant sind, wie Räumlichkeiten und Rechenzentren.

Dies bedeutet, dass das Testprogramm auch Sicherheit von Software, Code, Netzen, Cloud-Infrastrukturen, physischen Infrastrukturen usw. umfasst.



ANNERTON

Art. 24-25
DORA

# Resilienz-Testing

**Basistests**

- Das Basis-Testprogramm soll angemessene Tests umfassen, damit die Finanzunternehmen unter Anderem erkennen, wie sie auf IKT-Vorfälle vorbereitet sind und wo sie möglicherweise Schwachstellen in ihrer digitalen operationellen Resilienz haben.

- Tests müssen von **unabhängigen, internen oder externen Prüfern** durchgeführt werden.

- Für alle IKT-Systeme und -Anwendungen, die **kritische oder wichtige Funktionen** unterstützen, mindestens einmal jährlich angemessene Tests durchgeführt werden
  - Ausgenommen vom Resilienz-Testing: Kleinstunternehmen

- Finanzunternehmen müssen Verfahren und Leitlinien zur Priorisierung, Klassifizierung und Behebung aller während der Durchführung der Tests zutage getretenen Probleme und interne Validierungsmethoden festlegen

ANNERTON

# Sanktionen bei Nichteinhaltung

- **Verstoß gegen DORA ist Verstoß gegen Gesetz**
  - Umsetzung Sanktionsregime in DE durch FinmadiG:
  - Sicherstellung einer vorausschauenden und effektiven Aufsicht durch die Jahresabschlussprüfer, die die Einhaltung der DORA-Vorschriften prüfen und im Prüfbericht reflektieren
  - **z.B. Bußgeldkatalog in KWG:** Verstöße gegen DORA können mit Sanktionen von bis zu 5 Mio. EUR geahndet werden
  - weitreichende **Aufsichtsbefugnisse** der Behörden:
    - Maßnahmen und Bußgeldbescheide werden **veröffentlicht („**naming and shaming“)
    - erweiterte **Anordnungsbefugnis** der BaFin bei Verstößen gegen DORA (einschließlich Untersuchungen und Vorladung von Organmitgliedern)

ANNERTON

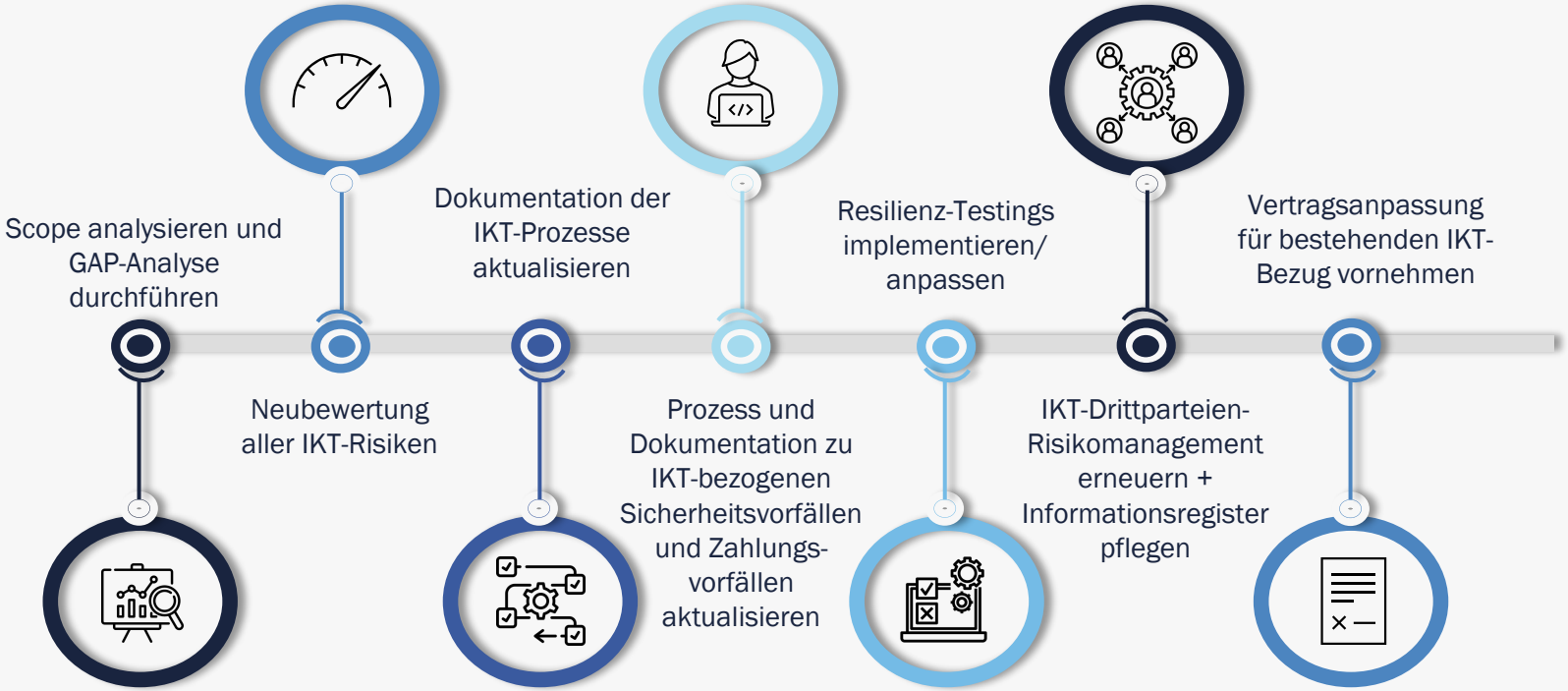

# Key Take-Aways:

## Auswirkungen des DORA für Investmentfonds & Wertpapierfirmen:

- ✓ gilt für KVGen und AIFs seit dem 17.01.2025, soweit keine Ausnahme; gilt ansonsten ggfs. ab dem 01.01.2027
- ✓ DORA bringt Akzentverschiebung der Aufsicht von finanzieller Leistungsfähigkeit hin zu operativer Resilienz durch starkes IKT-Risikomanagement
- ✓ IKT-Risikomanagement wird „Chefsache“
- ✓ mehr als 20 IKT-Risikomanagement-Themenbereiche, zu denen DORA inhaltliche Vorgaben macht und die über interne Richtlinien aktualisiert/angepasst werden müssen
- ✓ bestehende Verträge mit Dritten sind auf DORA anzupassen (Änderungsverhandlungen nötig)
- ✓ erheblich erhöhter Aufwand für das Führen und Aktualisieren des Informationsregisters
- ✓ umfassendes Testprogramm für alle IKT-Komponenten ist zu etablieren und zu dokumentieren
- ✓ Neue Funktionen: IKT-Risikomanager, IKT-Krisenkommunikationsmanager, IKT-Auslagerungsbeauftragter

ANNERTON

# Handlungsempfehlungen & Quick Wins



ANNERTON

# Handlungsempfehlungen

## GAP-Analyse durchführen

- DORA konkretisiert die bereits bestehenden Regulierungen und Standards zu den Anforderungen an die IT und erweitert sie in einem Umfang, der je nach Art des Unternehmens und dem bisher erreichten Reifegrad der Umsetzung der aktuellen regulatorischen Anforderungen an die IT einen erheblichen Umsetzungsbedarf auslöst.

**Tipp:** Listen Sie alle Anforderungen aus DORA und den RTS/ITS auf, ordnen Sie diese Anforderungen nach Kategorien/betroffenen Dokumenten/betroffenen Prozessen o.Ä. und prüfen Sie diese Anforderungen gegen bestehende Dokumentationen/Prozesse im Unternehmen.

ANNERTON

# Handlungsempfehlungen

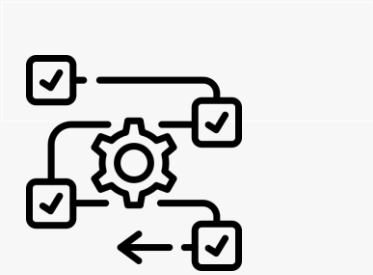
## Neubewertung aller IKT-Risiken

- Alle **IKT-Risiken müssen neu evaluiert** und in das gesamte Risikomanagementsystem von Instituten integriert werden.

- Dabei ist die Definition einer nachvollziehbaren, überschneidungsfreien und an die Risikoverteilung eines Instituts angepassten Risikotaxonomie/-methodik erfolgskritisch, damit z.B. die Zuordnung, Steuerung und Verantwortung für Informations- und Outsourcing-Risiken oder Cyber-Risiken klar definiert sind.

**Tipp:** Erfassen Sie alle IKT-Risiken im Unternehmen und berücksichtigen Sie dabei auch die Risiken, die in DORA und den RTS sowie in den Veröffentlichungen der Aufsicht (z.B. bei Cloud-Bezug) beschrieben sind. Bewerten Sie diese identifizierten Risiken im Rahmen einer neuen IKT-Risikoanalyse.

ANNERTON



# Handlungsempfehlungen

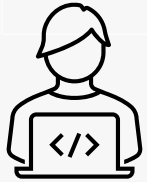
## Dokumentation der IKT-Prozesse aktualisieren

- Durch die RTS und ITS zu DORA ist klar, dass gerade im Bereich des IKT-Risikomanagements ein erheblicher Mehraufwand zur **Dokumentation der IKT-Prozesse und IKT-Systeme** erforderlich ist. So sieht der DORA-RTS zum IKT-Risikomanagementrahmen (Art. 15 DORA) mehr als 20 verschiedene interne IKT-bezogene Richtlinien (u.A. zum IKT Asset Management, zu Verschlüsselung und kryptografische Kontrollen, zum Kapazitäts- und Leistungsmanagement, zur Daten- und Systemsicherheit, zum Logging, zur Netzwerksicherheit, zum Change Management, zum Access Monitoring, zum Monitoring der IKT-Systeme, zum Management von IKT-bezogenen Sicherheitsvorfällen, zur IKT-bezogen Geschäftsfortführung im Krisenfall und zum Testen diverser Notfallpläne, aber auch zum Testen der IKT-Systeme) vor.

**Tipp:** Überprüfen Sie die bestehenden Dokumentationen im Bereich IKT im Hinblick auf Vollständigkeit und Aktualität und schließen Sie die in der GAP-Analyse identifizierten Lücken durch Update oder Neu-Erstellung der erforderlichen Dokumentationen. Die Einbeziehung des Leitungsorgans ist im Bereich IKT-Risikomanagment erheblich zu verstärken.

ANNERTON

# Handlungsempfehlungen



## Prozess und Dokumentation zu IKT-bezogenen Sicherheitsvorfällen

- Finanzunternehmen müssen gemäß Art. 17ff. DORA einen Prozess für die **Behandlung IKT-bezogener Vorfälle** entwickeln, um diese und erhebliche Cyberbedrohungen zu erkennen und zu mitigieren. Schwerwiegende IKT-bezogene Vorfälle (dies sind IKT-Vorfälle, die umfassende nachteilige Auswirkungen auf die Netzwerk- und Informationssysteme haben, die kritische oder wichtige Funktionen des Finanzunternehmens unterstützen) müssen an die BaFin und gegebenenfalls auch an Betroffene gemeldet werden.)

**Tipp**: Stellen Sie sicher, dass Ihre Richtlinien zum Incident Management allen DORA-Anforderungen entsprechen. Implementieren Sie eine Richtlinie zum Klassifizieren von Vorfällen und einen Incident Notfallplan mit klaren Rollen und Zuständigkeiten sowie Kommunikationsstrategien. Prüfen Sie, ob sie an das MVP-Portal der BaFin zur Abgabe von Meldungen über schwerwiegende IKT-Vorfälle angeschlossen sind.

ANNERTON

# Handlungsempfehlungen

## Resilienz-Testings implementieren/anpassen

- DORA fokussiert verstärkt auf der Prävention von IT- und Cyberbedrohungen und gibt daher konkrete Vorgaben für das Testen der digitalen operationalen Resilienz, die als integraler Bestandteil des IKT-Risikomanagements umgesetzt werden müssen.

- Hierzu sind **Anpassungen oder Neu-Implementierungen von Testing-Prozessen** und den entsprechend dazugehörigen Dokumentationen erforderlich.

**Tipp**: Identifizieren Sie die IKT-Assets, die Testings unterliegen und implementieren Sie regelmäßige Test-Zyklen für diese. Bei kritischen/wichtigen Funktionen sind mindestens jährliche Tests durchzuführen. Ordnen Sie allen ICT-Assets entsprechende Tests zu und entscheiden Sie, ob Sie die Tests durch interne oder externe Dritte durchführen lassen.

ANNERTON

# Handlungsempfehlungen

## IKT-Drittparteien-Risikomangement erneuern + Informationsregister pflegen

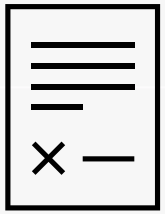
- Vor dem Vertragsschluss mit Dritten sind alle relevanten Risiken im Zusammenhang mit einer vertraglichen Vereinbarung über IKT-Bezug zu ermitteln und zu bewerten. Besonderes Augenmerk ist auf das IKT-Konzentrationsrisiko zu legen. Für die Auslagerung von kritischen/wichtigen Funktionen gelten besondere Anforderungen

- Das neue **IKT-Informationsregister** ist zu führen und erstmals bis zum 11.04.2025 an die BaFin zu melden
- .

**Tipp**: Passen Sie Ihre Auslagerungsrichtlinie an und entwickeln Sie eine Strategie für die Auslagerung von Dienstleistungen, die kritische/wichtige IKT-Funktionen unterstützen. Entwickeln Sie einen Due Diligence Prozess, um jeden IKT-Bezug vorab zu prüfen. Setzen Sie die Anforderungen an Form und Inhalt für das Informationsregister um, damit Sie Ihren Informationspflichten gegenüber der BaFin nachkommen können.

ANNERTON

# Handlungsempfehlungen



## Vertragsanpassung für bestehenden IKT-Bezug vornehmen

- Da DORA nicht zwischen Auslagerungen und sonstigem Fremdbezug von IKT-Dienstleistungen unterscheidet (sondern zwischen nicht-kritischen und kritischen/wesentlichen IKT-Funktionen), müssen die Mindestanforderungen an IKT-Verträge aus der DORA ggfs. auch auf Vertragsbeziehungen ausgerollt werden, die im aktuellen Auslagerungsregister nicht enthalten sind.

**Tipp**: Entwickeln Sie Vorlagen für zukünftige Verträge über IKT-Bezug und passen Sie Ihre bestehenden Verträge über IKT-Bezug an die neuen Anforderungen von DORA an. Legen Sie für IKT-Drittdienstleistungen ein gesondertes Informationsregister (zusätzlich/parallel zum Auslagerungsregister) an und nutzen Sie die Vorlagen/Vorgaben aus dem ITS zum Informationsregister dazu.

ANNERTON

# DORA –

## Resilience next level.

# Josefine Spengler

RECHTSANWÄLTIN
FACHANWÄLTIN FÜR IT-RECHT
COUNSEL

+49 30 863 2188 26
+49 175 325 06 30
jspengler@annerton.com

Als Fachanwältin für IT-Recht ist Josefine Spengler Spezialistin für alle aufsichtsrechtlichen Fragestellungen und Anforderungen an IT-Systeme im Zahlungsverkehr und für passgenaue Datenschutz-Konzepte im Unternehmen. Sie ist Expertin im IT- und FinTech-Segment und berät nationale und internationale Mandanten zu allen Fragestellungen an der Schnittstelle zwischen Aufsichtsrecht und IT-Recht, insbesondere zu DORA. Frau Rechtsanwältin Spengler verfügt über langjährige Erfahrung als Referentin und Autorin von Fachliteratur im Bereich IT-Aufsichtsrecht.

## Expertise

- IT-Anforderungen an Finanzunternehmen und regulierte Unternehmen
- IT-Recht/IT-Vertragsrecht
- DORA
- Outsourcing von IT
- IT-Richtlinien und -Dokumentationen
- Datenschutz im Unternehmen

ANNERTON


Annerton
Rechtsanwaltsgesellschaft mbH

Köthener Straße 2 – 3
D – 10963 Berlin
T +49 30 863 21 88 -0
F +49 30 863 21 88 -21
berlin@annerton.com

Annerton
Rechtsanwaltsgesellschaft mbH

Wöhlerstraße 5
60323 Frankfurt a. M.
T +49 69 2043 689 -0
F +49 69 2043 689 -99
frankfurt@annerton.com

Annerton
Rechtsanwaltsgesellschaft mbH

Wagmüllerstraße 23
D – 80538 München
T +49 89 306 683 -0
F +49 89 306 683 -212
munich@annerton.com

annerton.com