DORA, digitale Resilienz der Finanzunternehmen und ICT-Provider

– Ein erster Überblick und einige Details –

Roman Pusep

Rechtsanwalt, Fachanwalt für IT-Recht
Fachanwalt für Handels- und Gesellschaftsrecht

WERNER Rechtsanwälte Informatiker, Köln

Referent: RA Roman Pusep

- Partner, Rechtsanwalt
  Fachanwalt für IT-Recht
  Fachanwalt für Handels- und Gesellschaftsrecht
  Externer Datenschutzbeauftragter (TÜV-Zertifikat)

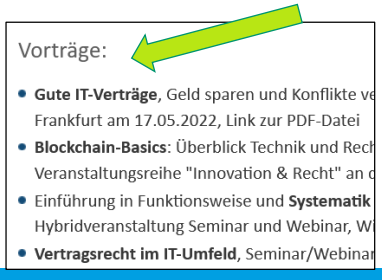
- **WERNER Rechtsanwälte Informatiker**
  Oppenheimstraße 16, 50668 Köln
- Telefon 0 221 / 97 31 43 – 73
  roman.pusep@werner-ri.de
  https://www.werner-ri.de

Die Präsentation

tech11

„Sehr“ juristische Inhalte für das Nacharbeiten ☺

- ... gibt es kostenlos und zur freien Verfügung
- ... unter der Website https://www.werner-ri.de
- ... unter „TEAM“ => „PARTNER“ => „Roman Pusep“
- ... und dann unten unter „VORTRÄGE“



Agenda

tech11

- **DORA – eine EU-Verordnung**
- **Ziele der DORA**
- **DORA-Umfeld**
- **Aufbau und Struktur der DORA**
- **Einige Details**
- **Handlungsfelder**

DORA – eine EU-Verordnung

tech11

- DORA
  - EN: digital operational resilience for the financial sector
  - DE: digitale operationale Resilienz im Finanzsektor
- VO (EU) 2022/2554

Bild generiert mit „being create“ →

DORA – eine EU-Verordnung

tech11

- Der Volltext
- https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32022R2554

VERORDNUNG (EU) 2022/2554 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 14. Dezember 2022

über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011

(Text von Bedeutung für den EWR)

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 114,

auf Vorschlag der Kommission,

nach Übermittlung des Entwurfs des Gesetzgebungsaktes an die nationalen Parlamente,

nach Stellungnahme der Europäischen Zentralbank (1),

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses (2),

gemäß dem ordentlichen Gesetzgebungsverfahren (3),

in Erwägung nachstehender Gründe:

DORA – eine EU-Verordnung

tech11

- **Exkurs:** Bedeutende EU-Rechtsakte
  - Verordnung
    - Art. 288 Abs. 2 AEUV:
    - Die Verordnung hat allgemeine Geltung. Sie ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.
  - Richtlinie
    - Art. 288 Abs. 3 AEUV:
    - Die Richtlinie ist für jeden Mitgliedstaat, an den sie gerichtet wird, hinsichtlich des zu erreichenden Ziels verbindlich, überlässt jedoch den innerstaatlichen Stellen die Wahl der Form und der Mittel.

DORA – eine EU-Verordnung

tech11

- **Exkurs:** EU-Verordnung
  - Europäisches Gesetz
  - Wirkt unmittelbar in jedem Mitgliedstaat
  - Erzeugt einheitliches EU-Recht => **Vollharmonisierung**
  - Geht nationalen Gesetzen grundsätzlich vor
    - es sein denn, eine Öffnungsklausel liegt vor
    - dann können Mitgliedstaaten ergänzende oder sogar abweichende Regelungen schaffen, je nach Öffnungsklausel

DORA – eine EU-Verordnung

tech11

- **Exkurs:** Öffnungsklausel (Beispiel)
  - Art. 2 Abs. 4 DORA:
    - Die **Mitgliedstaaten können** die in Art. 2 Abs. 5 Nr. 4 bis 23 der RiLi 2013/36/EU [Eigenkapitalrichtlinie] aufgeführten Stellen, die sich in ihrem jeweiligen Hoheitsgebiet befinden, **vom Geltungsbereich dieser Verordnung ausnehmen**. [...]
    - Art. 2 Abs. 5 Nr. 6 der RiLi 2013/36/EU: Diese Richtlinie findet keine Anwendung auf: [...] die Kreditanstalt für Wiederaufbau, Unternehmen, die aufgrund des Wohnungsgemeinnützigkeitsgesetzes als Organe staatlicher Wohnungspolitik anerkannt sind und nicht überwiegend Bankgeschäfte betreiben, und Unternehmen, die aufgrund dieses Gesetzes als gemeinnützige Wohnungsunternehmen anerkannt sind.

DORA – eine EU-Verordnung

tech11

- In-Kraft-Treten vs. Geltung/Anwendung
  - DORA wurde am 27. Dezember 2022 im EU-Amtsblatt veröffentlicht.
  - DORA ist am 17. Januar 2023 in Kraft getreten.
  - DORA gilt (= wird angewendet) ab 17. Januar 2025.
- Zitat aus Art. 64 DORA:
  - *Artikel 64*

    Inkrafttreten und Anwendung

    Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

    Sie gilt ab dem 17. Januar 2025.

Agenda

tech11

- **DORA – eine EU-Verordnung**
- **Ziele der DORA**
- **DORA-Umfeld**
- **Aufbau und Struktur der DORA**
- **Einige Details**
- **Handlungsfelder**

Ziele der DORA

tech11

- Das **Hauptziel** ergibt sich aus der Überschrift der Verordnung:
  - „Digitale **operationale Resilienz**“ oder in der Worten des Art. 1 Abs. 1 DORA:
    - Um ein **hohes gemeinsames Niveau** an digitaler operationaler Resilienz zu erreichen, werden in dieser Verordnung **einheitliche Anforderungen** für die Sicherheit von Netzwerk- und Informationssystemen, die die Geschäftsprozesse von Finanzunternehmen unterstützen, wie folgt festgelegt: [..]
  - Nach ErwG 1 DORA muss die Resilienz von IKT-Systemen
    - (1) erst noch besser **angegangen** werden und
    - (2) in den operativen Rahmen **integriert** werden.

Ziele der DORA

- Was bedeutet „Resilienz“?
  - DUDEN: psychische **Widerstandskraft**; Fähigkeit, schwierige Lebenssituationen ohne anhaltende Beeinträchtigung zu überstehen
  - Wiki: Resilienz (lateinisch resilire: zurückspringen, abprallen, nicht anhaften), auch Anpassungsfähigkeit, ist der **Prozess, in dem** Personen auf Probleme und Veränderungen mit Anpassung ihres Verhaltens reagieren. Dieser Prozess umfasst:
    - **Auslöser**, die Resilienz erfordern (z. B. Traumata oder Stress),
    - **Ressourcen**, die Resilienz begünstigen (z. B. Selbstwertgefühl, positive Lebenshaltung, unterstützendes soziales Umfeld) und
    - **Konsequenzen** (z. B. Veränderungen im Verhalten oder Einstellungen).

Agenda

- **DORA – eine EU-Verordnung**
- **Ziele der DORA**
- **DORA-Umfeld**
- **Aufbau und Struktur der DORA**
- **Einige Details**
- **Handlungsfelder**

DORA-Umfeld

tech11

- Bandbreite der Digital-Regularien

DORA-Umfeld

tech11

- Unterschiedliches Schicksal von Umfeld-Regularien
  - Während einige, unverbindliche Regularien nun **verbindlich werden sollen**, wie der TIBER-Standard für das Testing, welcher zusammen mit dem DORA-TLPT-RTS zum neuen Standard werden soll;
  - Sollen andere Regularien wiederum aufgrund der Redundanz **wegfallen**, wie die xAIT-Reihe,
    - vgl. Aufsichtsmitteilung DORA-Umsetzungshinweise BaFin vom 08. Juli 2024

„Gerüchte -Küche“

DORA-Umfeld

- DORA vs. **NIS-2**
  - Aktueller Entwurf des NIS-2-Umsetzungs-Gesetzes (16.08.2024)
    Link: https://dip.bundestag.de/vorgang/gesetz-zur-umsetzung-der-nis-2-richtlinie-und-zur-regelung-wesentlicher-grundz%C3%BCge/314976
  - § 28 Abs. 5 Nr. 1 BSI-Gesetz Entwurf:
    - **§§ 30, 31, 32, 35, 36, 38 und 39** (Risikomanagement, Unterrichtungs-, und Meldepflichten, Umsetzungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen) **gelten gilt nicht für Finanzunternehmen** nach Art. 2 Abs. 2 der VO (EU) 2022/2554 (DORA)
    - § 34 (Registrierungspflicht) u.a. gelten aber für Finanzunternehmen.
  - Begründung: Nach ErwG 28 NIS-2-RiLi gilt **DORA als lex specialis** für Finanzunternehmen, die von genannten NIS2-Pflichten ausgenommen sind.

Agenda

- **DORA – eine EU-Verordnung**
- **Ziele der DORA**
- **DORA-Umfeld**
- **Aufbau und Struktur der DORA**
- **Einige Details**
- **Handlungsfelder**

Aufbau und Struktur der DORA

tech11

- KAP. I Allgemeine Bestimmungen (Art. 1 bis 4)
- KAP. II **IKT-Risikomanagement** (Art. 5 bis 16)
- KAP. III Umgang, Klassifizierung, **Meldung** IKT-Vorfälle (Art. 16 bis 23)
- KAP. IV **Testen** der digitalen operationalen Resilienz (Art, 24 bis 27)
- KAP. V Management und Überwachungsrahmen des **IKT-Drittparteienrisikos** (Art. 28 bis 44)
- KAP. VI Vereinbarungen über Informationsaustausch (Art. 45)
- KAP. VII Zuständige Behörden (Art. 46 bis 56)
- KAP. VIII Delegierte Rechtsakte (Art. 57)
- KAP. IX Übergangs- und Schlussbestimmungen (Art. 58 bis 64)

Aufbau und Struktur der DORA

tech11

- **BaFin** benennt „**sechs wesentliche Bereiche**“
  - **IKT-Risikomanagement** (Kap. II, Art. 5 bis 16 DORA)
  - Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle (Kap. III, Art. 17 bis 23 DORA)
  - **Testen** der digitalen operationellen Resilienz einschließlich Threat-led Penetration Testing (TLPT) (Kap. IV, Art. 24 bis 27 DORA)
  - **IKT-Drittparteienrisiko-Management** (Kap. V, Art. 28 bis 30 DORA)
  - Überwachung kritischer IKT-Drittdienstleister (Kap. V, Art. 31 bis 44 DORA)
  - Vereinbarungen über Informationsaustausch sowie Cyberkrisen- und Notfallübungen (Kap. VI, Art. 44 und Kap. VII, Art. 49 DORA)

Quelle: https://www.bafin.de/DE/Aufsicht/DORA/DORA_node.html

Aufbau und Struktur der DORA

tech11

- Zusammenfassung der **Anforderungen** an Finanzunternehmen, **Art. 1 Abs. 1 lit. a) DORA**
  - **Risikomanagement** im Bereich der Informations- und Kommunikationstechnologie (IKT)
  - Maßnahmen für das solide **Management des IKT-Drittparteienrisikos**
  - **Tests** der digitalen operationalen Resilienz
  - **Meldung** (1) schwerwiegender IKT-bezogener Vorfälle und – freiwillig – erheblicher Cyberbedrohungen und (2) schwerer zahlungsbezogener Betriebs- oder Sicherheitsvorfälle an zuständige Behörden
  - **Austausch** von Informationen und Erkenntnissen in Bezug auf Cyberbedrohungen und Schwachstellen

Aufbau und Struktur der DORA

tech11

- **Adressaten** der DORA sind nach **Art. 2 Abs. 2 DORA**:
  - Finanzunternehmen und
  - IKT-Dienstleister
- **Finanzunternehmen sind (verkürzt):**
  - **Kreditinstitute**, **Zahlungsinstitute**, Kontoinformationsdienstleister, E-Geld-Institute, Wertpapierfirmen, Krypto-Dienste-Anbieter, Token-Emittenten, Zentralverwahrer, Handelsplätze, Transaktionsregister, Verwalter alternativer Investmentfonds, Verwaltungsgesellschaften, Datenbereitstellungsdienste, **Versicherungsunternehmen und -vermittler**, Einrichtungen betrieblicher Altersversorgung, Ratingagenturen, Schwarmfinanzierungsdienstleister, Administratoren kritischer Referenzwerte und Verbriefungsregister
  - **Achtung:** Ausnahmen für Kleinstunternehmen und größenabhängige Erleichterungen (Grundsätze der Angemessenheit und Proportionalität)

Aufbau und Struktur der DORA

tech11

- **Adressaten** der DORA sind nach **Art. 2 Abs. 2 DORA**:
  - Finanzunternehmen und
  - IKT-Dienstleister
- **IKT-Dienstleister – Definitionen:**
  - **Art. 3 Nr. 19 DORA:** „IKT-Drittdienstleister" sind Unternehmen, welche IKT-Dienstleistungen bereitstellen.
  - **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.

Aufbau und Struktur der DORA

tech11

- Adressaten der DORA – **Ausnahmekatalog, Art. 2 Abs. 3 DORA**:
  - Verwalter alternativer Investmentfonds (Art. 3 Abs. 2 RiLi 2011/61/EU)
  - Versicherungs-/Rückversicherungsunternehmen (Art. 4 RiLi 2009/138/EG)
  - Betrieblicher Altersversorger mit unter 15 Versorgungsanwärtern
  - Ausgenommene natürliche/juristische Personen (Art. 2, 3 RiLi 2014/65/EU)
  - **Rückversicherungsvermittler sowie Versicherungsvermittler (auch in Nebentätigkeit)**, soweit es Kleinst-, kleine oder mittlere Unternehmen sind
    - „kleinst": unter 10 Beschäftigte **und** max. 2 Mio. € Umsatz/Bilanzsumme
    - „kleine": unter 50 Beschäftigte **und** max. 10 Mio. € Umsatz/Bilanzsumme
    - „mittel": unter 250 Beschäftigte **und** max. 50/43 Mio. € Umsatz/Bilanz...
  - Postgiroämter (Art. 2 Abs. 5 Nr. 3 RiLi 2013/36/EU)

Aufbau und Struktur der DORA

tech11

- Ca. 70 **Definitionen**/Begriffe v.a. in Art. 3 DORA (ein Auszug)

Aufbau und Struktur der DORA

tech11

- Die Behörden:
  - Nationale Aufsicht – **BaFin**
  - Europäische Bankaufsichtsbehörde – **EBA**
  - Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung – **EIOPA**
  - Europäische Wertpapier- und Marktaufsichtsbehörde – **ESMA**

    ErwG 7 DORA: EBA + EIOPA + ESMA werden zusammen „Europäische Aufsichtsbehörden“ oder kurz „**ESA**“ genannt.

Aufbau und Struktur der DORA

tech11

- Die Hierarchie und die Sub-Strukturen
  - Level 1 Basisrechtsakt – DORA (EU-Rat und **EU-Parlament**)
  - Level 2 Delegierte Rechtsakte – Durchführungsstandards (**EU-Kommission**)
  - Level 3 Delegierte Rechtsakte – Standard-/Leitlinien-Vorbereitung **Aufsichtsbehörden** (ESAs)
- Auf Level 2 und Level 3 gibt es:
  - Delegierte Verordnung (**Del. VO**)
  - Technischer Regulierungsstandard (regulatory technical standard; **RTS**)
  - Durchführungsstandard (implementing technical standard; **ITS**)
  - (Gemeinsame) Leitlinien (guidelines; **GL**)

Aufbau und Struktur der DORA

tech11

- Beispiel für **Level 2 – RTS RMF**
  - Kommissions-Ermächtigung in der DORA
    - **Art. 15** UAbs. 4 und **Art. 16** Abs. 3 UAbs. 4 DORA: Der Kommission wird die Befugnis übertragen, DORA durch **technische Regulierungs-Standards** [...] zu ergänzen.
  - Delegierte Verordnung (EU) 2024/1774 der Kommission vom 13. März 2024
    - Art. 2 bis 18 – Richtlinien, Verfahren, Protokolle, Tools für IKT-Sicherheit
    - Art. 19 bis 21 – Richtlinien für Personalpolitik und Zugangskontrolle
    - Art. 22 bis 23 – Erkennung IKT-bezogener Vorfälle und Reaktion
    - Art. 24 bis 26 – Management der IKT-Geschäftsfortführung
    - Art. 27 – Bericht über Überprüfung des IKT-Risikomanagementrahmens

Aufbau und Struktur der DORA

tech11

- Beispiel für **Level 3 – TLPT RTS**
  - ESA-Beauftragung in **Art. 26 Abs. 11** DORA (Stufenmodell)
    - UAbs. 1: Die ESA arbeiten [mit EZB] im Einklang mit dem TIBER-EU-Rahmen gemeinsame Entwürfe technischer Regulierungsstandards aus, in denen Folgendes präzisiert wird: [...] Anforderungen und Standards für interne Tester, Umfang der TLPT, Testmethodik und Testkonzepte etc.
    - UAbs. 2: ESA berücksichtigt dabei Besonderheiten unterschiedlicher Art der Tätigkeiten in verschiedenen Finanzdienstleistungssektoren.
    - UAbs. 3: ESA übermitteln der Kommission diese Entwürfe technischer Regulierungsstandards bis zum 17. Juli 2024.
    - UAbs. 4: Der Kommission wird die Befugnis übertragen, DORA durch **technische Regulierungs-Standards** [...] zu ergänzen.

Aufbau und Struktur der DORA

tech11

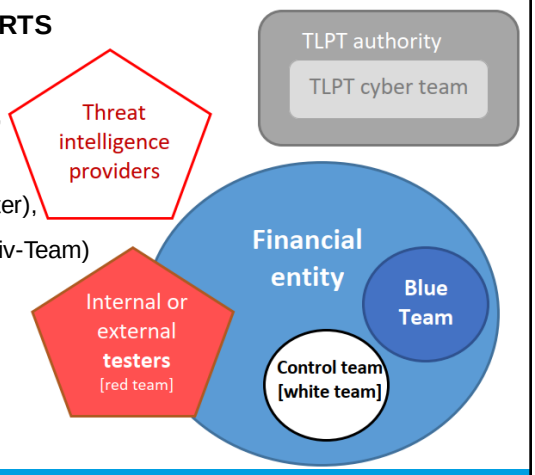
- Beispiel für **Level 3 – TLPT RTS**
  - Entwurf (Final Report) der ESAs vom 17. Juli 2024
    Kurztitel (nach BaFin): RTS zu Threat Led Penetration Testing (Art. 26 (11))
  - eba European Banking Authority | eiopa | ESMA

    186 Seiten
  - Aktiver Rotes-Teaming-Test dauert mind. 12 Wochen. Diese Dauer wird benötigt, um heimliche Bedrohungsakteure nachzuahmen (Ziffer 50)
  - Abgrenzung zwischen internen und externen Testern, z.B. gehört ein gruppeninterner IKT-Dienstleister zu internen Testern (Ziffer 71)
  - Bestimmung: gemeinsame TLPTs (Ziffer 78) vs. gepoolte TLPTs (Ziffer 80)
  - Anhänge, wie Projektcharta, Inhalte des Scope-Dokuments, Inhalte des Angriffsberichts, Testplan und Berichtsinhalte für rotes Team, etc.

Aufbau und Struktur der DORA

tech11

- Beispiel für **Level 3 – TLPT RTS**
  - Teamdefinitionen, wie
    - **white** team (Steuerung),
    - **blue** team (Ziel-Team),
    - **red** team (Angreifer/Tester),
    - **purple** team (Kollaborativ-Team)



Aufbau und Struktur der DORA

tech11

- Aktueller Status Level 2 und 3 (Stand: im Amtsblatt **veröffentlicht**)
  - RTS: Tools, Methoden, Prozesse, Richtlinien für **IKT-Risikomanagement** (Art. 15 und Art. 16 Abs. 3) – (Nr. 2024/1774: „RTS RMF“)
  - RTS: **Vertragsinhalte** für externe IKT-Dienstleistungen für kritische oder wichtige Funktionen (Art. 28 Abs. 10) – (Nr. 2024/1773: „RTS TPPol“)
  - RTS: **Klassifizierungs-Kriterien** IKT-bezogener **Vorfälle** und Cyber-bedrohungen (Art. 18 Abs. 4) – (Nr. 2024/1772)
  - Del. VO: Kriterien für die **Einstufung** von IKT-Drittdienstleistern für Finanzunternehmen **als kritisch** (Art. 31 Abs. 6) – (Nr. 2024/1502)
  - Del. VO: Höhe der von federführender Überwachungsbehörde bei kritischen IKT-Drittdienstleistern zu erhebenden **Überwachungsgebühren** und Entrichtung dieser Gebühren (Art. 43 Abs. 2) – (Nr. 2024/1505)
    (Hinweis: umsatzbezogen, jedoch mind. 50.000,--€,)

Aufbau und Struktur der DORA

tech11

- Aktueller Status Level 2 und 3 (Stand: ESA's **Entwurf**)
  - RTS: **TLPT** – Threat Led Penetration Testing (Art. 26 Abs. 11 DORA)
  - RTS: Spezifizierung von zu bewertenden Elementen bei **Untervergabe** von IKT-Dienstleistungen (Art. 30 Abs. 5 DORA)
  - RTS: Inhalte der **Meldung** schwerwiegender IKT-Vorfälle und erheblicher Cyberbedrohungen sowie Meldefristen schwerer Vorfälle (Art. 20. a) DORA)
  - IST: Standardformulare, **Vorlagen**, Verfahren **zur Meldung** schweren IKT-bezogenen Vorfalls oder erheblicher Cyberbedrohung (Art. 20. b) DORA)
  - GL: Geschätzte **Kosten und Verluste durch** schwerewiegende IKT-bezogene **Vorfälle** (Art. 11 Abs. 11 DORA)
  - IST: Standardvorlage für **Informationsregister** (Art. 28 Abs. 9 DORA)
  - GL: **Zusammenarbeit** zwischen ESAs und Behörden (Art. 32 Abs. 7)

Agenda

tech11

- **DORA – eine EU-Verordnung**
- **Ziele der DORA**
- **DORA-Umfeld**
- **Aufbau und Struktur der DORA**
- **Einige Details – kleine Auswahl**
- **Handlungsfelder**

Details – Leitungsverantwortung

tech11

- Leitungsorgan/Geschäftsleitung
  - Governance nach Art. 5 DORA: Das Leitungsorgan … (verkürzt)
    - trägt letztendliche **Verantwortung** für IKT-Risiko-Management
    - führt Leitlinien für hohe **Standards** ein
    - legt klare IKT-Aufgaben und -**Verantwortlichkeiten** fest
    - trägt Gesamtverantwortung für **Strategie** digit. operationaler Resilienz
    - genehmigt, überwacht und überprüft die Umsetzung der **IKT-Leitlinie**
    - genehmigt und überprüft regelmäßig die internen **IKT-Revisionspläne**
    - weist angemessene **Budgetmittel** zu
    - richtet auf Unternehmensebene **Meldekanäle** ein

Details – Leitungsverantwortung

tech11

- Leitungsorgan/Geschäftsleitung
  - Governance nach Art. 5 DORA: Das Leitungsorgan … (verkürzt)
    - richtet Überwachungsfunktion für **Verträge mit IKT-Dienstleistern** ein
    - hält **Kenntnisse** und **Fähigkeiten** aktiv auf neuestem Stand, und zwar durch spezielle Schulungen
    - genehmigt das Verfahren für das IKT-Änderungsmanagement (Art. 9 Abs. 4 UAbs. 3 DORA)
    - lässt sich von leitenden IKT-Mitarbeitern mind. jährlich über Tests und Vorfälle berichten und Empfehlungen geben (Art. 13 Abs. 5 DORA)
    - überprüft regelmäßig Risiken im Zusammenhang mit Verträgen über die Nutzung von IKT-Dienstleistungen (Art. 28 Abs. 2 DORA)

Details – Leitungsverantwortung

tech11

- Leitungsorgan/Geschäftsleitung
  - Konsequenzen:
    - Leitungsorgane sind Adressaten von verwaltungsrechtlichen **Sanktionen** und Abhilfemaßnahmen (Art. 50 Abs. 5 DORA)
    - Ergo: Auch **Geschäftsführer/Vorstand Haftung**
  - **Ferner**:
    - Wirtschaftsprüfer geben Jahresabschluss/Bilanz nicht frei
    - Probleme mit Kunden, Lieferanten und anderen Partnern

Das Geschäft mit der Angst

Details – DOR-Strategie

tech11

- Strategie für die digitale operationale Resilienz
  - DOR-Strategie erforderlich, Detailvorgaben in **Art. 6 Abs. 8 DORA**
  - **IT-Notfallmanagement** nicht explizit genannt, anders in xAIT
    - Aber: IT-Notfallmanagement bei IKT-Dienstleistern, Art. 28 Abs. 8 DORA
  - Bestimmte **Standards** werden in der DOR-Strategie nicht gefordert (so wie noch z.B. in Ziffer 1.2 BAIT), allerdings werden sie von der Kommission nahegelegt (vgl. Art. 2 Abs. 2 lit. h) RTS RMF). Danach sind „führende Praktiken und gegebenenfalls Normen zu berücksichtigen."
  - Neuer Begriff: „**IKT-Referenzarchitektur**". Keine Definition in Art. 3 DORA; ein einziges Mal genannt: in Art. 6 Abs. 8 lit. d) DORA.
  - BaFin: **Akzentverschiebung von** (bloßer) **Informationssicherheit zum** (risikobasierten) **IKT-Risikomanagement**

Details – IKT-Governance-/-Kontrollrahmen

tech11

- IKT-Governancerahmen und -Kontrollrahmen
  - **Unabhängige Überwachung** der IKT-Risiken, Art. 6 Abs. 4 DORA, einschl.
    - Vermeidung von Interessenkonflikten sowie
    - Trennung und Unabhängigkeit von IKT-Risikomanagementfunktionen, Kontrollfunktionen und internen Revisionsfunktionen
  - Anforderungen an die Richtlinien für IKT-Sicherheit, Art. 2 Abs. 2 RTS RMF:
    - Datum der Genehmigung durch das Leitungsorgan
    - Verantwortlichkeiten der Beschäftigten auf allen Ebenen
    - Folgen einer Nichteinhaltung durch Beschäftigte
    - Verzeichnis der erforderlichen Dokumentation
    - führende Praktiken und gegebenenfalls Normen

… und einiges mehr !

Details – Moderne IT

tech11

- Stand der Technik
  - Der Begriff „Stand der Technik“ fehlt, aber Verpflichtung besteht.
  - ErwG 48 DORA: Wegen sich rasch ändernder Bedrohungslage „sollten“ Finanzunternehmen **auf dem neuesten Stand befindliche IKT-Systeme** unterhalten, die zuverlässig sind und nicht nur die Verarbeitung der für die Erbringung ihrer Dienste erforderlichen Daten, sondern auch ausreichende technologische Resilienz gewährleisten, um auf ungünstige Umstände reagieren zu können.
  - Art. 5 Abs. 2 lit. b) DORA: Leitlinien sollen **hohe Standards** der **Integrität**, **Verfügbarkeit**, **Authentizität** und **Vertraulichkeit** von Daten sicherstellen.
  - Art. 7 DORA: Um IKT-Risiken zu bewältigen und zu managen, verwenden und unterhalten **Finanzunternehmen stets auf dem neuesten Stand zu haltende IKT-Systeme, -Protokolle und -Tools**, die [... Anforderungen ...]

Details – Moderne IT

- **IT-Systeme müssen** folgende Eigenschaften stets aufweisen (nach Art. 7 DORA):
  - Angemessen dimensioniert sein,
  - Zuverlässig funktionieren,
  - Auftragsspitzen bearbeiten können,
  - Technologieneuerungen/-wechsel bewältigen,
  - **Technologisch resilient** sein, um einem erforderlichen zusätzlichen Bedarf an Informationsverarbeitung angemessen zu begegnen, z.B.
    - unter angespannten Marktbedingungen oder
    - unter anderen widrigen Umständen.

Details – Moderne IT

- Änderungen von IT-Systemen
  - Art. 9 Abs. 4 lit. e) DORA:
    - Es sind zu implementieren und dokumentieren **Richtlinien, Verfahren und Kontrollen** für das **IKT-Änderungsmanagement**, einschließlich Änderungen an Software, Hardware, Firmware-Komponenten, den Systemen oder von Sicherheitsparametern, die auf einem Risiko-Bewertungsansatz basieren und fester Bestandteil des gesamten Änderungsmanagementprozesses sind, um sicherzustellen, dass **alle Änderungen** an IKT-Systemen auf kontrollierte Weise erfasst, getestet, bewertet, genehmigt, implementiert und überprüft werden.
  - Anmerkung der BaFin (Umsetzungshinweise, 08.07.2024):
    - **Bisherige Betrachtung** beschränkte sich auf wesentliche Änderungen, diese Einschränkung ist künftig nicht mehr vorgesehen.

Details – Moderne IT

tech11

- Entwicklung (und Wartung sowie Beschaffung) von IT-Systemen
  - Art. 16 Abs. 1 RTS RMF:
    - **Richtlinien für** die Beschaffung, die **Entwicklung** und die Wartung sind zu entwickeln, zu dokumentieren und zu implementieren.
  - Richtlinien müssen Anforderungen enthalten an:
    - Sicherheitskonzepte und Methoden für Entwicklung ...
    - Angaben von technischen Spezifikationen vorsehen
    - Angaben von Anforderungen an die IKT-Sicherheit vorsehen
    - Genehmigungsverfahren
    - Maßnahmen, um Manipulationsrisiko während der Entwicklung, Wartung und Einführung zu mindern

Details – Das Prüfen und Testen

tech11

- Test-Überblick (nach ErwG 56 + Art. 25 Abs. 1 DORA)
  - Lückenanalysen / **Schwachstellenscans**
  - Analysen von Open-Source-Software
  - Bewertungen der Netzwerksicherheit
  - Analysen der physischen Sicherheit
  - Fragebögen und Scansoftwarelösungen
  - Quellcodeprüfungen, soweit möglich
  - **Penetration-Test** (Cybersicherheit) = szenariobasiert und risikobasiert
  - Backup/Restore-Test
  - Disaster-Recovery-Test

Art. 10 Abs. 1 DORA: *Finanzunternehmen haben* ***Mechanismen****, um […] potenzielle wesentliche* ***Schwachstellen*** *zu finden.*

Details – Das Prüfen und Testen

tech11

- Jährliche Überprüfungen von ...
  - IKT-**Risikomanagement**rahmen, häufiger anlassbezogen (Vorfälle, Tests) (Art. 6 Abs. 5 DORA)
  - **Klassifizierung** der IKT-gestützten Unternehmensfunktionen, Rollen und Verantwortlichkeiten, die Informations- und IKT-Assets (Art. 8 Abs. 1 DORA)
  - **Risikoszenarien**: Risiken gegenüber und von anderen Finanzunternehmen sowie Cyberbedrohungen und IKT-Schwachstellen (Art. 8 Abs. 2 DORA)
  - Spezifische Bewertung des IKT-Risikos bei **IKT-Altsystemen**, häufiger bei Anschluss von Technologien, Anwendungen/Systemen (Art. 8 Abs. 7 DORA)
  - IKT-Geschäftsfortführungs**pläne** sowie IKT-Reaktions**pläne** und Wiederherstellungs**pläne** bei IKT-Systemen (Art. 11 Abs. 6 DORA)
  - **IKT-Systeme** von kritischer/wesentlicher Bedeutung (Art. 25 Abs. 6 DORA)

Details – Das Prüfen und Testen

tech11

- TIBER EU und TIBER DE
  - ECB: **TIBER**-EU (**T**hreat **I**ntelligence-**B**ased **E**thical **R**ed Teaming), Mai 2018
  - Bundesbank, BMF, BaFin: Implementierung von TIBER-DE, Dezember 2022
    - Dokument Version 3.0
    - Quelle: https://www.bundesbank.de/de/aufgaben/unbarer-zahlungsverkehr/tiber-de/tiber-de-816986
    - Zielgruppe: große Banken und **große Versicherer**, aktive Finanzmarktinfrastrukturen sowie aktive kritische IT-Dienstleister

Details – Das Prüfen und Testen

tech11

- TIBER EU und TIBER DE
  - Bundesbank, BMF, BaFin: Implementierung von TIBER-DE, Dezember 2022
    - Phasen:
      - Vorbereitungsphase: Initiierung, Kick-Off, Bestimmung des Testumfangs und Beschaffung
      - Testphase: Sammlung von Informationen zur Bedrohungslage (ca. 6 Wochen) und Durchführung des Red Team Tests (ca. 12 Wochen)
      - Abschlussphase: Testberichte, Replay, Purple Teaming und Feedback, Behebungsplan und Abschlussbericht
  - BaFin: **TIBER-DE wird durch DORA zur Pflicht**. (27.02.2024) https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2024/fa_bj_2402_DORA.html

Details – Das Prüfen und Testen

tech11

- Externe und interne Tester
  - Art. 26 Abs. 1 DORA: **mindestens alle drei Jahre** anhand von TLPT erweiterte Tests durchführen.
    - Zuständige Behörde kann anhand Risikoprofils und betrieblicher Gegebenheiten die Häufigkeit verringern oder erhöhen.
  - Art. 26 Abs. 2 DORA:
    - Getestet wird das **Live-Produktionssystem**.
    - Schutzmaßnahmen planen, umsetzen, prüfen und dokumentieren
  - Art. 26 Abs. 8 UAbs. 1 DORA
    - Wenn Finanzunternehmen interne Tester für die Durchführung von TLPT einsetzen, dann müssen sie **alle drei Tests externe Tester** beauftragen.

Details – IKT-Dienstleister

- **Vertragsinhalte** – Regelungen
  - DORA
    - Art. 30 DORA – Wesentliche Vertragsbestimmungen
  - Delegierte Verordnung:
    - RTS: **Vertragsinhalte** für externe IKT-Dienstleistungen für kritische oder wichtige Funktionen (Art. 28 Abs. 10) – (Nr. 2024/1773: „RTS TPPol“)

Details – IKT-Dienstleister

- **Vertragsinhalte** – Beispiele (Grundsatzregelungen)
  - **Klare, zweifelsfreie, transparente und dokumentierte Verpflichtungen**
  - Klare, vollständige Beschreibung **aller** Funktionen und IKT-Dienstleistungen
  - Bestimmungen über **Unterauftragnehmer** für kritische/wichtige Funktionen
  - **Standorte** der Bereitstellung, Verarbeitung, Speicherung – Änderungsinfo!
  - Bestimmungen über **Verfügbarkeit**, Authentizität, Integrität, Vertraulichkeit
  - Sicherstellung des Datenzugangs bei **Insolvenz** des IKT-Dienstleisters
  - Dienstleistungs**güte**, einschließlich Aktualisierungen und Überarbeitungen
  - Handlungspflichten beim IKT-Vorfall; **ohne Zusatz-/Überraschungskosten**
  - Kündigungsrechte und Mindestkündigungsfristen

Details – IKT-Dienstleister

- **Vertragsinhalte** – Beispiele (kritische/wichtige Funktionen)
  - Umfassende Regelung zur Qualität (= Dienstleitungsgüte), um wirksame Überwachung und Eingreifen sicherzustellen – **Monitoring**
  - Meldung aller Entwicklungen, die das Leistungsniveau betreffen
  - Notfallpläne implementieren und testen, einschließlich TLPT
  - Überprüfungsbefugnisse:
    - Zugangs-, Inspektions- und Auditrechte
    - Uneingeschränkte Zusammenarbeit bei Behörden-Vor-Ort-Inspektionen
    - Herausgabe von Audit-Berichten

Details – IKT-Dienstleister

- **Vertragsinhalte** – Beispiele (kritische/wichtige Funktionen)
  - **EXIT-Szenarien**
    - Änderung, Abwicklung und Umstrukturierung sicherstellen
    - **Anbieterwechsel und Insourcing** ermöglichen
  - ErwG 66 DORA:
    - Betreffen vertragliche Vereinbarungen kritische oder wichtige Funktionen, so sollten Finanzunternehmen darauf achten, dass IKT-Drittdienstleister die **aktuellsten und höchsten Standards für die Informationssicherheit** anwenden.

Details – IKT-Dienstleister

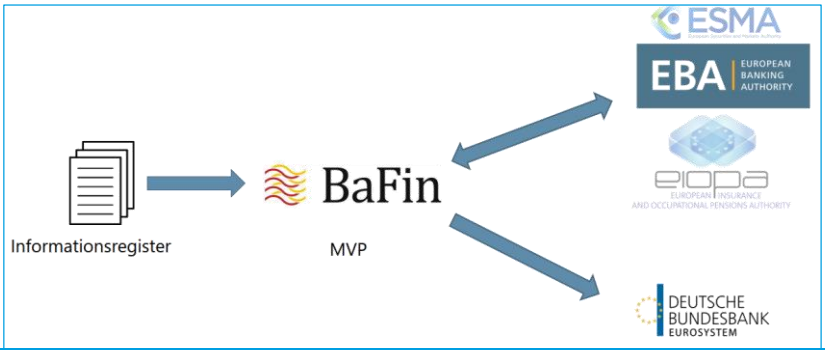
tech11

- **Informationsregister**
  - Art. 28 Abs. 3 UAbs. 1 DORA:
    - Finanzunternehmen führen und aktualisieren im Rahmen ihres IKT-Risikomanagementrahmens auf Unternehmensebene sowie auf teilkonsolidierter und konsolidierter Ebene ein **Informationsregister, das sich auf alle Vereinbarungen über die Nutzung von durch IKT-Drittdienstleister bereitgestellten IKT-Dienstleistungen** bezieht.
  - Art. 28 Abs. 3 UAbs. 4 DORA:
    - Finanzunternehmen **stellen der zuständigen Behörde auf Verlangen** das **vollständige Informationsregister** oder auf Anfrage bestimmte Teile dieses Registers **zusammen mit allen Informationen** zur Verfügung, die für eine wirksame Beaufsichtigung als notwendig erachtet werden.

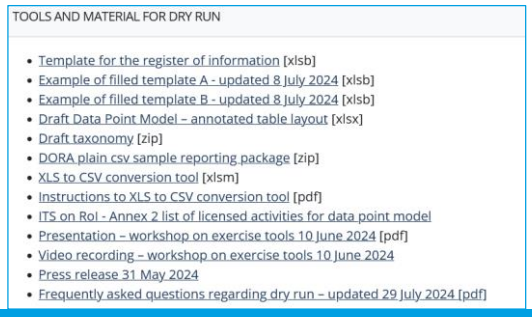
Details – IKT-Dienstleister

tech11

- **Informationsregister**
  - Meldeweg nach Präsentation der BaFin vom 21.06.2024:



Details – IKT-Dienstleister

- **Informationsregister**
  - ESA-Informationen https://www.eba.europa.eu/activities/direct-supervision-and-oversight/digital-operational-resilience-act/preparation-dora-application
  - 
TOOLS AND MATERIAL FOR DRY RUN

- Template for the register of information [xlsb]
- Example of filled template A - updated 8 July 2024 [xlsb]
- Example of filled template B - updated 8 July 2024 [xlsb]
- Draft Data Point Model – annotated table layout [xlsx]
- Draft taxonomy [zip]
- DORA plain csv sample reporting package [zip]
- XLS to CSV conversion tool [xlsm]
- Instructions to XLS to CSV conversion tool [pdf]
- ITS on RoI - Annex 2 list of licensed activities for data point model
- Presentation – workshop on exercise tools 10 June 2024 [pdf]
- Video recording – workshop on exercise tools 10 June 2024
- Press release 31 May 2024
- Frequently asked questions regarding dry run – updated 29 July 2024 [pdf]

… sehr viel und nützlich

Details – IKT-Dienstleister

- **Überwachungsrahmen** für kritische IKT-Drittdienstleister
  - Geregelt in: Art. 31 ff. DORA
  - **Direkte Überwachung durch Aufsichtsbehörden** und zwar zusätzlich zu den Überwachungspflichten der Finanzunternehmen
  - Warum?
    - ErwG 28 Satz 1 DORA: Bei Nutzung von IKT-Dienstleistungen haben Finanzunternehmen **häufig Schwierigkeiten**, Vertragsbedingungen auszuhandeln, die Aufsichtsstandards oder -anforderungen genügen.
  - Beispiel für kritischen IKT-Drittdienstleister :
    - ErwG 20 Satz 2 DORA: Der DORA-Überwachungsrahmen gilt für alle kritischen IKT-Drittdienstleister, inkl. **Anbieter von Cloud-Computing-Diensten**, die Finanzunternehmen IKT-Dienstleistungen bereitstellen.

Details – IKT-Dienstleister

- **Überwachungsrahmen für kritische IKT-Drittdienstleister**
  - ErwG 98 DORA: EU-Kommission soll/wird
    - die **Einstufung** von IKT-Drittdienstleistern **als kritisch** weiter quantifizieren und präzisieren,
    - systemische **Auswirkungen eines Ausfalls** eines Dienstes oder eines IKT-Drittdienstleisters präzisieren,
    - die Anzahl global systemrelevanter Institute (G-SRI) oder anderer systemrelevanter Institute (A-SRI) bestimmen,
    - die Überwachungs**gebühren** und Zahlungsweise harmonisieren und
    - hierzu delegierte Rechtsakte (Art. 290 AEUV) zur DORA-Ergänzung erlassen (Art. 28 Abs. 10 UAbs. 3 DORA); auch hier aufgrund der ESA-Vorlage (Art. 28 Abs. 10 UAbs. 1 DORA)

Agenda

- **DORA – eine EU-Verordnung**
- **Ziele der DORA**
- **DORA-Umfeld**
- **Aufbau und Struktur der DORA**
- **Einige Details – kleine Auswahl**
- **Handlungsfelder**

Handlungsfelder

tech11

Und nun ??
- Nachdenken
- Handeln

- Handlungsfelder **erkennen und priorisieren** ausgehend von **wesentlichen Bereichen**
  - IKT-Risikomanagement (inkl. **VAIT-GAP**) ★ ★ ★ ★
  - IKT-Drittparteienrisiko-Management ★ ★ ★ ★
  - Resilienz-Testung, inkl. (TLPT) ★ ★ ★
  - Meldewesen IKT-bezogene Vorfälle ★ ★
  - Informationsaustausch ★
- Finanzunternehmen sind **nicht allein**
  - DORA ist ein Segen für **IT-Dienstleister** 😇

tech11

Vielen Dank !

Empfehlen Sie uns weiter!

WERNER | R | I
RECHTSANWÄLTE
INFORMATIKER

https://www.werner-ri.de