BaFin

Bundesanstalt für
Finanzdienstleistungsaufsicht

DORA

Europäischer Verordnungsentwurf zur digitalen operationalen Resilienz im Finanzsektor

Silke Brüggemann, Referat GIT 3
Grundsatz IT-Aufsicht und
Aufsichtsunterstützung

Digital Operational Resilience Act (DORA)

- Digital Finance Package

  Veröffentlichung des Verordnungsentwurfs nebst zugehöriger Änderungsrichtlinie am 24. September 2020 durch die Europäische Kommission

- Zielsetzung

  Stärkung der digitalen operationalen Resilienz durch einheitliche Regeln für den gesamten Finanzsektor

EUROPEAN COMMISSION

Brussels, XXX
COM(2020) 595/2

2020/0266 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014

(Text with EEA relevance)

{SWD(2020) 198} - {SWD(2020) 199}

EN EN

Digital Operational Resilience Act (DORA)

Wesentliche Elemente

- Harmonisierung des IKT-Risikomanagements (IKT-Governance und IKT-Risikomanagement-Rahmenwerk)
- Vereinheitlichung und Ausweitung der Meldepflichten von schwerwiegenden IKT-Vorfällen auf den gesamten Finanzsektor
- Europäisches Oversight Framework für kritische IKT-Drittdienstleister

Weitgefasster Anwendungsbereich:

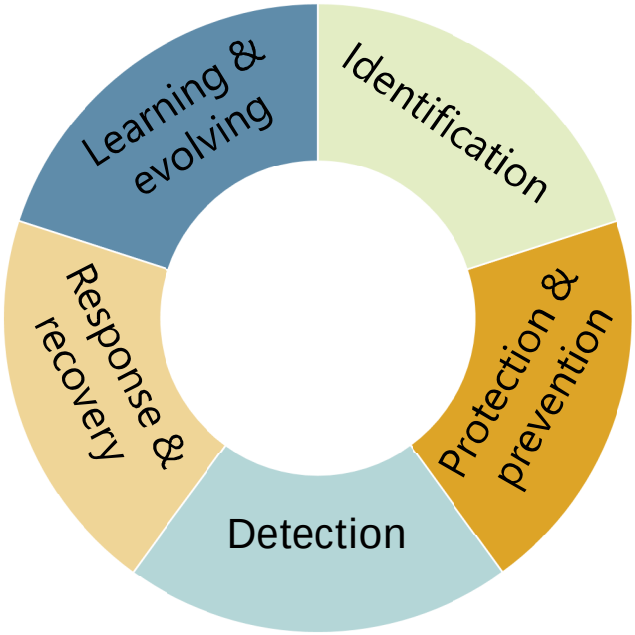
- Kreditinstitute
- Zahlungsdienstleister
- Erst- und Rückversicherungs-unternehmen & EbAV
- Wertpapierfirmen
- E-Geld-Institute
- „Kryptoverwahrer“
- Central Securities Depositories (CSD)
- Zentrale Gegenparteien
- Handelsplätze
- ...

IKT-Governance & IKT-Risikomanagement-Rahmenwerk

- Harmonisierte und einheitliche Prinzipien
- IKT-Governance & Organisation

  Gesamtverantwortung der Geschäftsleitung als allumfassendes Prinzip
- IKT-Risikomanagement-Rahmenwerk
  - Orientierung am NIST Framework for Improving Critical Infrastructure Cybersecurity
  - Vorgehensweise: Standardneutrale und risikoorientierte Umsetzung
  - Ziel: Aufrechterhaltung & Wiederherstellung der Funktionsfähigkeit des Finanzunternehmens
- DORA macht vsl. eine Anpassung der einschlägigen Leitlinien der ESAs notwendig

Elemente IKT-Risikomanagement



Testen der digitalen operationalen Resilienz

- Basistests

  Etablierung eines risikobasierten Testprogramms, bspw. Schwachstellentests

- Fortgeschrittene Tests
  - Threat Led Penetration Testing (TLPT)
  - Anforderung nur für signifikante Finanzunternehmen
  - Orientierung an TIBER-EU
  - Austausch & Anerkennung der Testergebnisse zwischen den europäischen Aufsichtsbehörden

IKT-Vorfallsmeldepflichten

- Vereinheitlichung und Ausweitung der Meldepflichten von schwerwiegenden IKT-Vorfällen auf den gesamten Finanzsektor
  - Nationale Aufsichtsbehörde als alleinige Empfängerin
  - Informationsweitergabe an ESAs, EZB und BSI
  - Delegierung der Meldung von Vorfällen nach Genehmigung der NCA
- Förderung des Informationsaustausches

IKT-Drittparteienrisikomanagement

- Risikoorientiertes Management der IKT-Drittparteienrisiken
- Informationsregister & jährliche Übermittlung an NCA
- Risikoanalyse
- Wesentliche Vertragsbestandteile, bspw.:
  - Beschreibung des Vertragsgegenstandes
  - Verpflichtung des Vertragspartners, bei IKT-Vorfällen Unterstützung zu leisten
  - Ausstiegsstrategie

Oversight Framework für kritische IKT-Drittdienstleister

- Kriterien

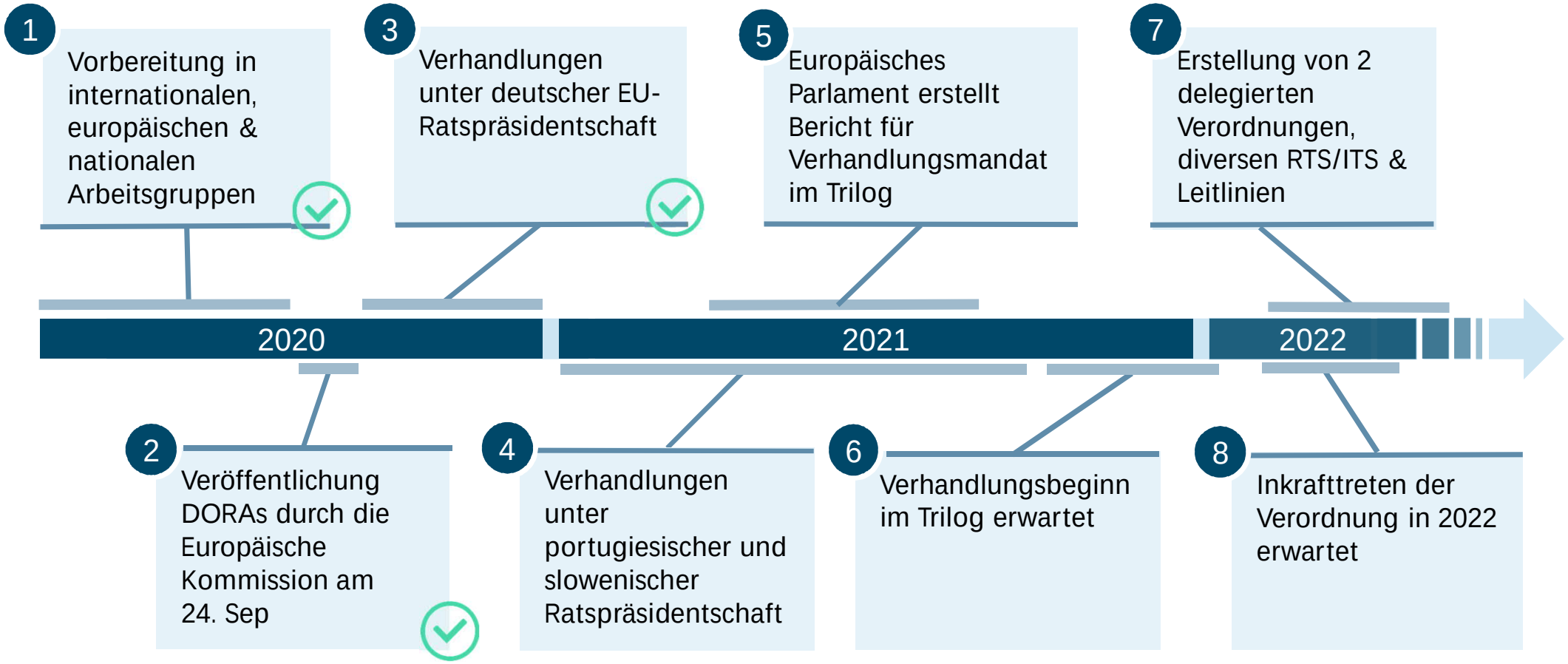
  Systemische Risiken für den Finanzsektor

- Governance

  - Lead Overseer: EBA/ESMA/EIOPA
  - Joint Examination Teams von NCAs und ESAs
  - Oversight Forum: ESAs und NCAs beratend

- Informations-, Kontroll- und Prüfrechte durch Lead Overseer
- Sitz in der EU für kritische IKT-Drittdienstleister zwingend, aber keine verpflichtende Datenhaltung innerhalb der EU

Aktuelles und nächste Schritte



Fragen?

Bildnachweis: pixabay.com/geralt