BaFin

Bundesanstalt für
Finanzdienstleistungsaufsicht

DORA

Europäischer Verordnungsentwurf zur digitalen operationalen Resilienz im Finanzsektor

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

Agenda

- Digital Operational Resilience Act (DORA)
- Informations- und Kommunikationstechnologie (IKT)-Governance & IKT-Risikomanagement
- Testen der digitalen operationalen Resilienz
- IKT-Vorfallsmeldepflichten
- IKT-Drittparteirisikomanagement
- Oversight Framework für kritische IKT-Drittdienstleister
- Vergangenes, Aktuelles und nächste Schritte

Digital Operational Resilience Act (DORA)

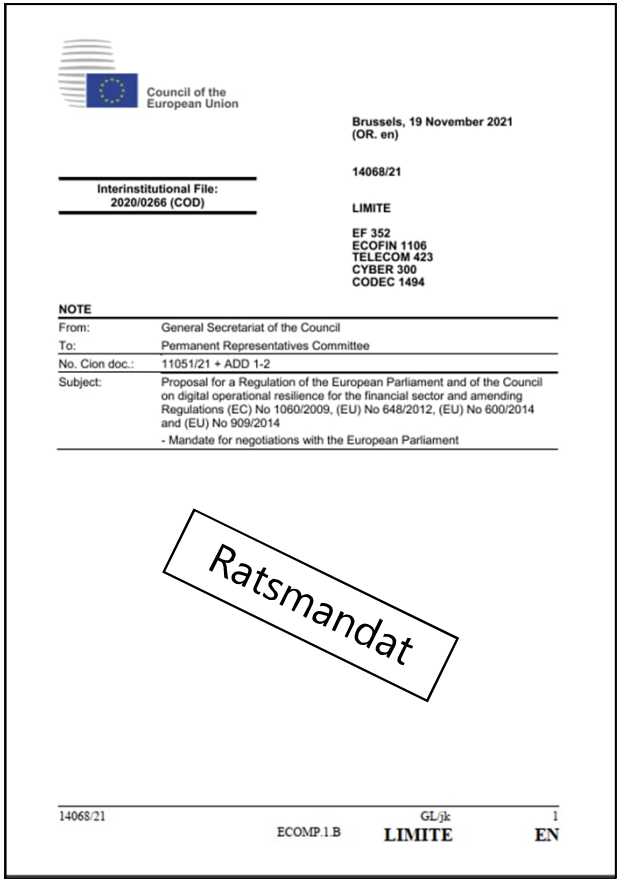
- Digital Finance Package

  Veröffentlichung Verordnungsentwurf und Änderungsrichtlinie durch die Europäische Kommission, 24. September 2020

- Verhandlungsmandate Rat und Parlament

  Vorlage Ende 2021

- Zielsetzung
  - Stärkung der digitalen operationalen Resilienz
  - Einheitliche Regeln
  - Gesamter Finanzsektor



Council of the European Union

Brussels, 19 November 2021
(OR. en)

14068/21

Interinstitutional File:
2020/0266 (COD)

LIMITE

EF 352
ECOFIN 1106
TELECOM 423
CYBER 300
CODEC 1494

NOTE

From:	General Secretariat of the Council
To:	Permanent Representatives Committee
No. Cion doc.:	11051/21 + ADD 1-2
Subject:	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 - Mandate for negotiations with the European Parliament

Ratsmandat

14068/21 GL/jk 1
ECOMP.1.B LIMITE EN

Digital Operational Resilience Act (DORA)

Wesentliche Elemente

- Einheitliches und harmonisiertes IKT-Risikomanagement-Rahmenwerk
- Ausweitung und Vereinheitlichung der Meldepflichten von schwerwiegenden IKT-Vorfällen auf den gesamten Finanzsektor
- Europäisches Oversight Framework für kritische IKT-Drittdienstleister

Weitgefasster Anwendungsbereich:

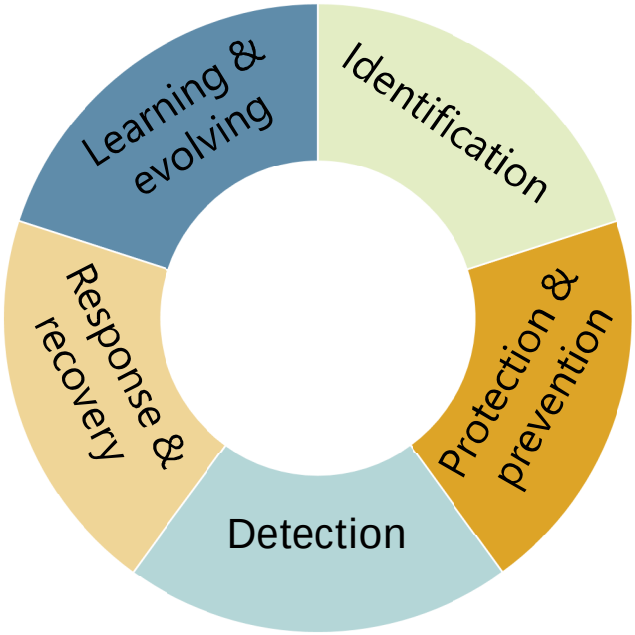
- Erst- und Rückversicherungs-unternehmen
- Einrichtungen betrieblicher Altersvorsorge
- Versicherungs- und Rückversicherungsvermittler
- Kreditinstitute
- Zahlungsdienstleister
- Wertpapierfirmen
- „Kryptoverwahrer“
- ...

Ausnahmen vorhanden

IKT-Governance & IKT-Risikomanagement

- IKT-Governance & Organisation
  - Harmonisierte und einheitliche Prinzipien
  - Gesamtverantwortung der Geschäftsleitung als allumfassendes Prinzip
- IKT-Risikomanagement
  - Element des IKT-Risikomanagement-Rahmenwerks
  - Aufrechterhaltung & Wiederherstellung der Funktionsfähigkeit des Finanzunternehmens
  - Standardneutrale, proportionale und risikoorientierte Umsetzung
- Anpassung der einschlägigen Leitlinien der europäischen Aufsichtsbehörden (ESAs)

Elemente IKT-Risikomanagement



Testen der digitalen operationalen Resilienz

Element des IKT-Risikomanagement-Rahmenwerks

Basistests

Etablierung eines risikobasierten Testprogramms

Fortgeschrittene Tests

- Threat Led Penetration Testing (TLPT)
- Anforderung nur für bedeutende Finanzunternehmen
- Orientierung am Rahmenwerk TIBER-EU (Threat Intelligence-based Ethical Red Teaming)
- Austausch & Anerkennung der Testergebnisse zwischen den europäischen Aufsichtsbehörden

IKT-Vorfallsmeldepflichten

- Ausweitung und Vereinheitlichung der Meldepflichten von schwerwiegenden IKT-Vorfällen auf den gesamten Finanzsektor
  - Zuständige Behörde als Empfängerin
  - „Lex specialis“-Klausel – Verhältnis zur Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS-Richtlinie)
  - Informationsweitergabe an die europäischen Aufsichtsbehörden (ESAs) und das Bundesamt für Sicherheit in der Informationstechnik (BSI)

- Förderung des Informationsaustausches

IKT-Drittparteirisikomanagement

- Element des IKT-Risikomanagement-Rahmenwerks

- Risikoorientiertes Management der IKT-Drittparteirisiken

- Informationsregister

- Risikoanalyse

- Wesentliche Vertragsbestandteile, zum Beispiel:
  - Beschreibung des Vertragsgegenstandes
  - Verpflichtung des Vertragspartners, bei IKT-Vorfällen Unterstützung zu leisten
  - Ausstiegsstrategie

Oversight Framework für kritische IKT-Drittdienstleister

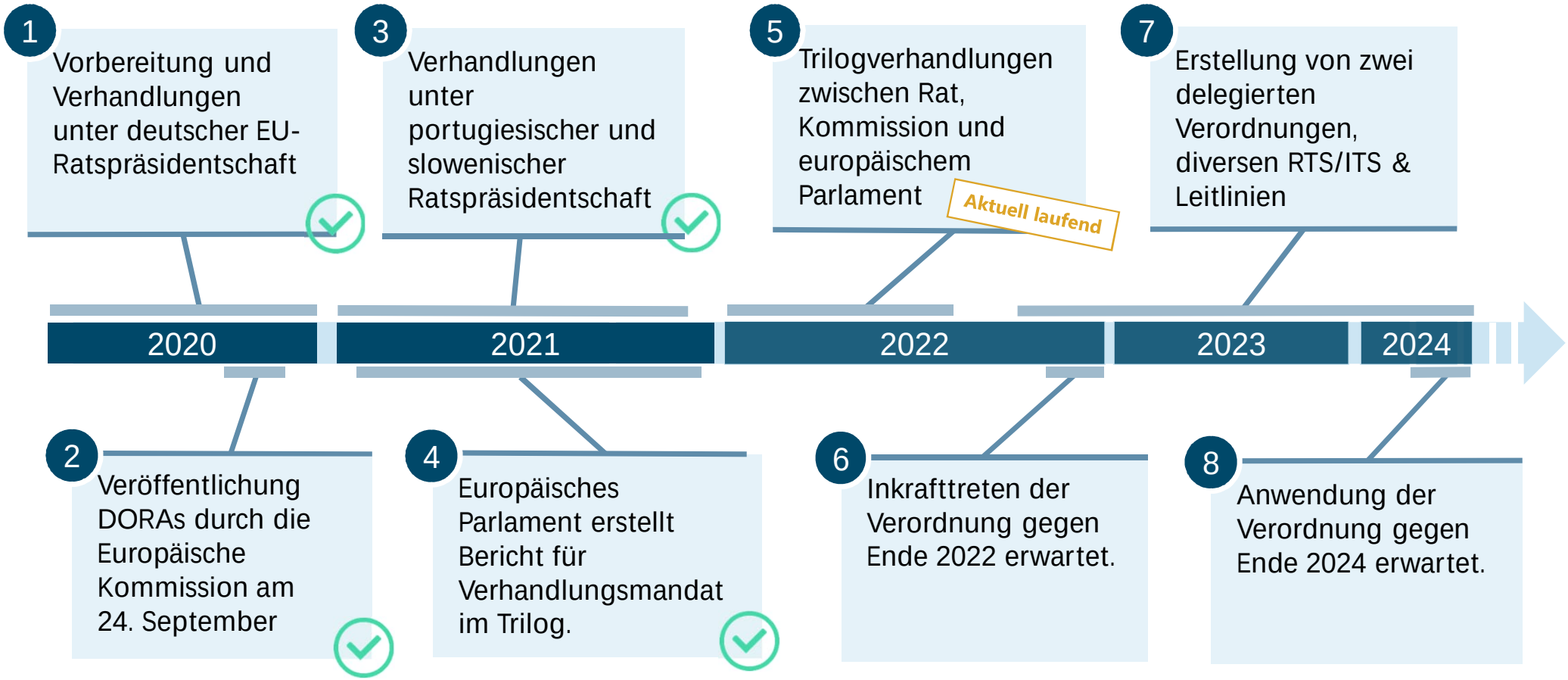
- Kriterien
  - Systemische Risiken für den Finanzsektor

- Governance
  - Lead Overseer: EBA/ESMA/EIOPA
  - Joint Examination Teams, zusammengesetzt aus Expertinnen und Experten der zuständigen Behörden und der europäischen Aufsichtsbehörden (ESAs)
  - Oversight Forum: ESA und zuständige Behörden

- Informations-, Kontroll- und Prüfrechte durch Lead Overseer

- Sitz in der EU für kritische IKT-Drittdienstleister zwingend

Vergangenes, Aktuelles und nächste Schritte



Silke Brüggemann
Referat GIT 3
Grundsatz IT-Aufsicht und Aufsichtsunterstützung
Telefon: +49(0)228 4108-1405
E-Mail: silke.brueggemann@bafin.de

Bildnachweis: pixabay.com/geralt