

# BarCamp

Regulatorik am Beispiel DORA (Digital Operational Resilience Act)

14. Dezember 2022

# BarCamp – 14.12.2022 15-20 Uhr

Regulatorik am Beispiel DORA (Digital Operational Resilience Act)






**Moderator**  
**Axel Dors**



**Moderatorin**  
**Sarah Richter**

# Regulatoren

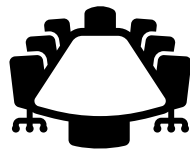
	<b>International</b>	<b>• Basler Ausschuss für Bankenaufsicht</b>	
	Europa	<ul style="list-style-type: none"><li>• EU-Kommission</li><li>• Europäisches Parlament</li><li>• Rat der Europäischen Union</li></ul>	<ul style="list-style-type: none"><li>• Europäische Bankenaufsichtsbehörde (EBA)</li><li>• Europäische Zentralbank (EZB)</li></ul>
	Deutschland	<ul style="list-style-type: none"><li>• Bundesregierung</li><li>• Bundestag</li><li>• Bundesrat</li></ul>	<ul style="list-style-type: none"><li>• Bundesanstalt für Finanzaufsicht (BaFin)</li><li>• Deutsche Bundesbank</li></ul>

# Regulatoren

## Europäische Union



EU-Richtlinien und EU-Verordnungen



EU-  
Kommission



Europäisches  
Parlament



Rat der  
Europäischen  
Union

# Regulatoren

## Europäisches Finanzaufsichtssystem (ESFS) seit 01.01.2011



## Europäischen Aufsichtsbehörden (ESA)



# DORA

- 1. Lesung im EU-Parlament im November 2022
- Aktuelle Version vom 17.11.2022  
<https://data.consilium.europa.eu/doc/document/t/PE-41-2022-INIT/DE/pdf>
- Verabschiedung voraussichtlich im 1. Halbjahr 2023
- Gilt ab 24 Monate nach Inkrafttreten der Verordnung  
(voraussichtlich ab Mitte 2025)

**VERORDNUNG (EU) 2022/...  
DES EUROPÄISCHEN PARLAMENTS UND DES RATES**

vom ...

**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) Nr. 2016/1011**

**(Text von Bedeutung für den EWR)**

# DORA: Artikel 2: Geltungsbereich

- a) Kreditinstitute
- b) Zahlungsinstitute
- c) Kontoinformationsdienstleister
- d) E-Geld-Institute
- e) Wertpapierfirmen
- f) Anbieter von Krypto-Dienstleistungen
- g) Zentralverwahrer
- h) zentrale Gegenparteien
- i) Handelsplätze
- j) Transaktionsregister
- k) Verwalter alternativer Investmentfonds
- l) Verwaltungsgesellschaften
- m) Datenbereitstellungsdienste
- n) Versicherungs- und Rückversicherungsunternehmen
- o) Versicherungsvermittler, Rückversicherungsvermittler und Versicherungsvermittler in Nebentätigkeit
- p) Einrichtungen der betrieblichen Altersversorgung
- q) Ratingagenturen
- r) Administratoren kritischer Referenzwerte
- s) Schwarmfinanzierungsdienstleister
- t) Verbriefungsregister
- u) IKT-Drittdienstleister

# DORA: Inhalt

- Kapitel I Allgemeine Bestimmungen
- Kapitel II: IKT-Risikomanagement
  - Abschnitt I
  - Abschnitt II
- Kapitel III: Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle
- Kapitel IV: Testen der digitalen operationalen Resilienz
- Kapitel V: Management des IKT-Drittparteienrisikos
  - Abschnitt I: Schlüsselprinzipien für ein solides Management des IKT-Drittparteienrisikos
  - Abschnitt II: Überwachungsrahmen für kritische IKT-Drittanbieter
- Kapitel VI: Vereinbarung über den Austausch von Informationen
- Kapitel VII: Zuständige Behörden
- Kapitel VIII: Delegierte Rechtsakte
- Kapitel IX: Übergangs- und Schlussbestimmungen



# Austausch





**ISACA®**

Germany Chapter