

Blog Post

N° 1/2020

DORA - Digital Operational Resilience Act

EU-Verordnung für digitale Resilienz im Finanzsektor

Dr. Andreas Windisch

ASQUARED

asquared Blog Post N° 1/2020

September 2020

Copyright © asquared GmbH

Der Digital Operational Resilience Act (DORA) wurde im September 2020 von der EU-Kommission vorgeschlagen, um die digitale Widerstandsfähigkeit des Finanzsektors zu stärken. Banken, Versicherungen, Zahlungsdienstleister und ihre IT-Dienstleister müssen künftig strenge Vorgaben zu Risikomanagement, Vorfallmeldungen und Auslagerungen erfüllen. Da DORA spätestens 2025 verbindlich wird, ist es entscheidend, dass Unternehmen sich frühzeitig mit den Anforderungen befassen.

Wer oder was ist DORA?

Am 24. September 2020 veröffentlichte die EU-Kommission den Verordnungsvorschlag zur digitalen operativen Resilienz im Finanzsektor, bekannt als **Digital Operational Resilience Act (DORA)**, Teil des "Digital Finance"-Pakets der EU. Ziel ist es, die Fragmentierung der Cyber- und IT-Risikovorschriften in der Finanzbranche zu beenden und erstmals einheitliche, sektorübergreifende Mindestanforderungen an die digitale Resilienz von Finanzdienstleistungsunternehmen zu schaffen

Wen betrifft die Verordnung?

Der Entwurf sieht vor, dass alle Finanzunternehmen im Binnenmarkt direkt erfasst werden, ohne vorherige nationale Umsetzung, darunter Banken, Versicherungen, Investmentfirmen usw. Auch IKT-Drittanbieter (Anbieter von Informations- und Kommunikationstechnologie), insbesondere solche mit systemischer Bedeutung, werden adressiert: Die Verordnung sieht vor, dass kritische Drittanbieter besondere Anforderungen erfüllen und einer EU-weiten Aufsicht unterliegen können.

Was sind die Kernelemente der Verordnung?

Der DORA-Verordnungsentwurf strukturiert sich entlang zentraler Anforderungen:

- 1 **IKT-Risikomanagement** – Finanzakteure sollen über ein robustes Framework verfügen, um Risiken aus Informationstechnologie systematisch zu managen.
- 2 **Meldung von IKT-bezogenen Vorfällen** – Einheitliche Schwellenwerte und Taxonomien sollen eingeführt werden, um gravierende IT-Störungen zu identifizieren und zu melden.
- 3 **Operational Resilience Testing** – Der Vorschlag fordert regelmäßige Tests, um Schwachstellen zu identifizieren und Resilienz zu gewährleisten.

- 4 **Risikomanagement bei Drittanbietern** – Einschließlich Due Diligence, Überwachung und Regelungen für Auslagerungen an ICT-Dienstleister.
- 5 **Informationsaustausch über Cyber-Bedrohungen und Zwischenfälle** – um sektorenweite Abwehr zu stärken

Was müssen betroffene Unternehmen tun?

Es liegen zwar noch keine finalen Vorgaben vor, aber der Entwurf signalisiert stark in Richtung klarer Pflichten:

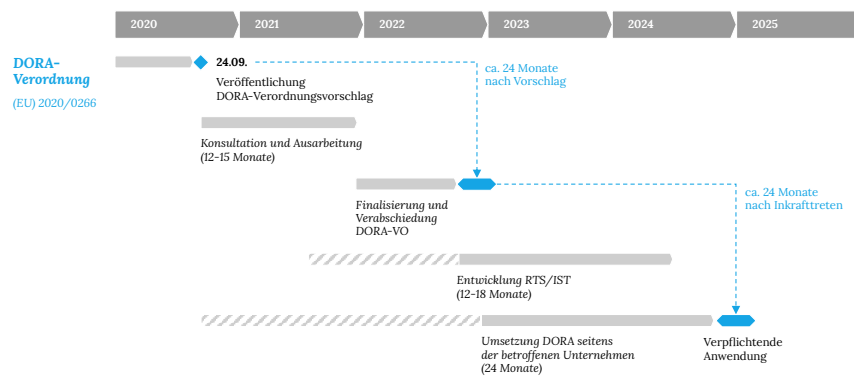
- Aufbau oder Anpassung eines IKT-Risikomanagement-Frameworks; Governance und Strategie für digitale Resilienz.
- Einrichtung eines Vorfallmanagements mit Meldewegen und Schwellenwerten für IKT-Vorfälle.
- Regelmäßige Tests, z. B. auf Liefersicherheit oder Belastungsszenarien.
- Überprüfung und Vertragsgestaltung gegenüber ICT-Drittanbietern, insbesondere im Bereich Cloud oder kritischer Infrastruktur.
- Aufbau oder Beteiligung an Informationsnetzwerken zum Cyber-Threat-Sharing.

All das im Bewusstsein, dass kleinere Unternehmen proportional entlastet werden können – zum Beispiel durch einen "vereinfachten IKT-Risikomanagementrahmen".

Welche Timeline gilt es zu beachten?

DORA ist ein vielversprechender Verordnungsvorschlag, der den digital bedingten Risiken im Finanzsektor EU-weit einen kohärenten, einheitlichen Rahmen geben soll. Mit Fokus auf IKT-Risiken, Incident-Reporting, Resilienz-Tests, Drittanbieter-Oversight und Cybersharing will DORA regulatorische Fragmentierung beenden und die Widerstandsfähigkeit der Finanzinstitute stärken.

Die EU strebt eine zügige Verabschiedung und Umsetzung an – wenngleich Details zur konkreten Umsetzungszeit, Detailvorgaben und Aufsichten noch ausstehen, lassen die gängigen zeitlichen Umsetzungshinweise die Konstruktion einer groben Timeline zu. Abbildung 1 illustriert den anzunehmenden zeitlichen Rahmen von heute bis zur verpflichtenden Anwendung der regulatorischen Anforderungen voraussichtlich Ende 2024 bzw. Anfang 2025.



Quelle: asquared / Stand September 2020

ASQUARED

Abbildung 1: DORA-Verordnung: Übersicht voraussichtliche Timeline

Für Finanzinnovatoren und IT-Verantwortliche bedeutete das: Die Weichen technologisch und organisatorisch zu stellen – im Bewusstsein, dass bald verpflichtende Pflichten rund um IKT-Resilienz auf EU-Ebene eingeführt werden.

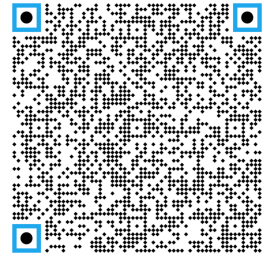
Quellenangaben

- 1 Europäische Kommission, „Proposal for a Regulation on digital operational resilience for the financial sector (COM/2020/595 final)“, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52020PC0595>
- 2 Europäische Kommission, „Explanatory Memorandum to the Proposal for a Regulation on digital operational resilience (Impact Assessment)“, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52020PC0595>
- 3 Europäische Kommission, „Impact Assessment Report accompanying the DORA proposal (SWD(2020)198 final)“, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52020PC0595>

Autoren



Dr. Andreas Windisch ist Managing Director bei asquared. Er ist Diplom-Informatiker und promovierter Ingenieur. Er wirkte in leitenden Positionen bei Automobil-, Technologie- und Beratungsunternehmen und verfügt über langjährige Erfahrungen im Bereich des IT-Transformationsmanagements im Automobil- und Finanzdienstleistungssektor.



Über asquared

Asquared ist eine Unternehmensberatung aus Berlin. Mittelpunkt der Arbeit ist die Erarbeitung praktischer Lösungsansätze für den regulatorisch, technologisch und/oder gesellschaftlich induzierten Wandel, verbunden mit der jeweilig unmittelbaren Anwendung und Bestätigung im industriellen Umfeld.

Unser Augenmerk liegt stets auf Business und Technologie und ihrem Wechselspiel. Von der Neuausrichtung der Strategie, über das (Re)Design von Produkten und Services bis hin zur Operationalisierung – wir gestalten die Veränderung. Auf allen Ebenen.

Ausgewählte Erkenntnisse dieser theoretischen und praktischen Forschungsarbeiten stellen wir in Form von Publikationen und Fachvorträgen einer breiteren Öffentlichkeit zur Verfügung.

asquared GmbH


Pappelallee 78/79


10437 Berlin - Deutschland

Telefon +49 (0) 30 22 66 79 60


E-Mail contact@asquared.team

 [asquared.company](https://www.asquared.company)

 [asquared.blog](https://www.asquared.blog)

 twitter.com/asquaredgmbh

 [instagram.com/asquaredgmbh](https://www.instagram.com/asquaredgmbh)

 [linkedin.com/company/asquared](https://www.linkedin.com/company/asquared)