

DORA Digital Operational Resilience Act

Die Europäische Union hat mit DORA, der Verordnung (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor (Digital Operational Resilience Act), eine umfassende Regulierung für den Finanzsektor in Bezug auf Cybersicherheit, IKT-Risiken und digitale operationale Resilienz eingeführt.

Was ist DORA?

Ende September 2020 veröffentlichte die EU-Kommission die Initiative zur “Digital Operational Resilience” als Teil eines Maßnahmenpakets zur **Digitalisierung des Finanzsektors**. Das Hauptziel dieser Initiative ist es, die Wettbewerbsfähigkeit, Innovation sowie Resilienz und Cyber-Sicherheit zu stärken. Die DORA-Verordnung trat am 16. Januar 2023 in Kraft und setzt eine Frist von zwei Jahren für die Umsetzung ihrer Bestimmungen.

Der Vorschlag erweitert die **bestehenden Vorschriften** (wie MaRisk/MaGo/KAMaRisk, BAIT/VAIT/KAIT usw.) und legt einen besonderen Schwerpunkt auf die Anforderungen in Bezug auf Cyber- und weitere digitale Risiken.

Zu den **Schlüsselementen** gehören die Harmonisierung der Vorschriften für das Risikomanagement der Informations- und Kommunikationstechnologie (IKT), die Meldung von Sicherheitsvorfällen, Tests und Prüfungen sowie die Berichterstattung und das Management von IT-Drittanbietern.



Worauf zielt DORA ab?

DORA zielt darauf ab, die digitale operationale Widerstandsfähigkeit von EU-Finanzunternehmen und ihren IKT-Drittdienstleistern zu verbessern und einen EU-weit einheitlichen Aufsichtsrahmen zu schaffen. Die Anfälligkeit für Cyberbedrohungen und IKT-Störungen soll über die gesamte Wertschöpfungskette des Finanzsektors reduziert werden.

Regulierungsstandards (RGS und ITS):

Diese werden in den ab November 2023 veröffentlicht. Der Fokus liegt auf der Notwendigkeit der Umsetzung.

Governance:

- Strategie für digitale operationale Resilienz (Art. 9)
- Verantwortlichkeit des Leitungsorgans (Art. 5)

Testverfahren: Unternehmen sind verpflichtet, regelmäßige Tests durchzuführen, um ihre Fähigkeit zu gewährleisten, allen Arten von IKT-bezogenen Störungen und Bedrohungen standzuhalten, darauf zu reagieren und sich davon zu erholen.

- Bedrohungs-basierte Penetrationstests (Art. 26–27)
- Testen der Wiederherstellungspläne Resilienz (Art. 24–25)
- Testen der Wiederherstellungspläne (Art. 11)

Management des IKT-Drittparteirisikos: Unternehmen müssen das Risiko von IKT-Drittparteien, die ihnen Dienstleistungen im Bereich IKT wie Cloud-Plattformen oder Datenanalysedienste bereitstellen, effektiv managen.

- IKT-Drittparteienstrategie (Art. 28)
- Vertragsgestaltung und Risikoanalyse (Art. 28, 30)
- Informationsaustausch (Art. 28)
- Ausstiegsstrategien (Art. 28, 30)

IKT-bezogene Vorfälle: Unternehmen müssen ihre kritischen Funktionen und Vermögenswerte identifizieren, klassifizieren und dokumentieren. Sie müssen alle Quellen von IKT-Risiken kontinuierlich überwachen, um Schutz- und Präventionsmaßnahmen aufzubauen. Zudem müssen sie IKT-bezogene Vorfälle melden und dokumentieren.

- Erkennung, Klassifizierung und Benachrichtigung von Vorfällen (Art.10 , Art .7–10)
- Reaktion auf IKT-Vorfälle (Art .11)
- Kommunikation (Art .11 &14)

Erfahrungen nutzen

Die isacon AG ist Ihr vertrauenswürdiger Begleiter auf dem Weg zur Einhaltung der DORA EU-Verordnung 2022/2554. Unser Expertenteam steht bereit, um Sie bei der Planung und Umsetzung Ihrer Projekte zu unterstützen, um die Anforderungen der DORA-Verordnung zu erfüllen. Wir nehmen uns die Zeit, Ihre spezifischen Bedürfnisse zu verstehen und entwickeln maßgeschneiderte Lösungen, die auf die DORA-Verordnung abgestimmt sind. Zögern Sie nicht, uns zu kontaktieren. Wir freuen uns darauf, mit Ihnen zusammenzuarbeiten.



Strategien der BANK AG zur Erfüllung der DORA EU-Verordnung: Ein umfassender Ansatz zur operationellen Resilienz

Nehmen wir an, die BANK AG, eine der größten Banken in Deutschland, stünde vor der Herausforderung, die Anforderungen von **DORA** zu erfüllen. Die Bank hat bereits eine **robuste IT-Infrastruktur** und **Prozesse**, aber DORA erfordert eine noch umfassendere Herangehensweise an die operationelle Resilienz.



Zunächst könnte die BANK AG ihre **IT-Governance-Struktur** überarbeiten, um sicherzustellen, dass sie über wirksame Maßnahmen zur operationellen Resilienz verfügt. Dies könnte beinhalten, dass sie einen speziellen Ausschuss oder eine Abteilung einrichtet, die sich ausschließlich mit Fragen der **operationellen Resilienz** befasst.

Darüber hinaus könnte die BANK AG ein **geeignetes Risikomanagement** implementieren, um das Risiko von IKT-Drittparteien zu managen. Dies könnte beinhalten, dass sie strenge Kontrollen und Überprüfungsprozesse für ihre IKT-Drittanbieter einführt, um sicherzustellen, dass diese die Anforderungen von DORA erfüllen.

Die BANK AG könnte auch **regelmäßige Tests** durchführen, um ihre Fähigkeit zu gewährleisten, allen Arten von IKT-bezogenen Störungen und Bedrohungen standzuhalten, darauf zu reagieren und sich davon zu erholen. Dies könnte beinhalten, dass sie regelmäßige **Penetrationstests** und andere **Sicherheitstests** durchführt, um Schwachstellen in ihren Systemen zu identifizieren und zu beheben.

Unsere Experten helfen Ihnen weiter!

Die isacon AG kann als Partner dienen, um Ihre Geschäftsprozesse zu verbessern, neue Anwendungen zu erstellen und bestehende Systeme zu verbinden. Wir bieten professionelle Beratung und Installation, um die DORA-Anforderungen zu erfüllen. Die genauen Schritte hängen von der spezifischen Situation und den Bedürfnissen der Bank ab.



Dr. Andreas Klein

 andreas.klein@isacon.com

 +49 (173) 72 682 60 / +49 (6201) 259 65 0

 isacon AG
Bergstraße 49 / 69469 Weinheim