Digital Operational Resilience Act

Warum Sie jetzt handeln sollten

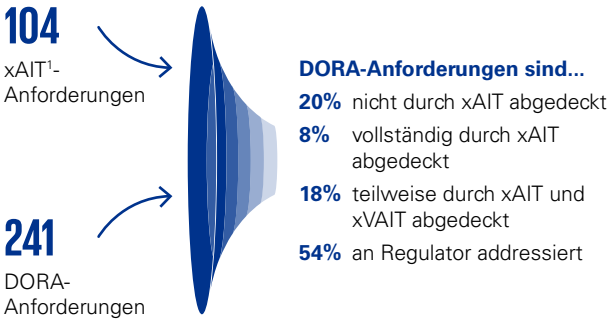
Der Digital Operational Resilience Act („DORA“) vereinheitlicht bestehende europäische und nationale Standards und Anforderungen und schafft somit einen Rahmen für die digitale Betriebsstabilität von europäischen Finanzunternehmen. Der Schwerpunkt liegt auf der Aufrechterhaltung des (digitalen) Geschäftsbetriebs und der damit verbundenen Prozesse sowie Dienstleistungen. Wichtige Bestandteile sind die Harmonisierung der Vorschriften für das Risikomanagement von Informations- und Kommunikationstechnologien (IKT), für die Berichterstattung und für die Risikobewertung von IKT-Drittanbietern.

Timeline DORA

- **seit 2020:**
  - Vorbereitung und Verhandlungen unter deutscher EU-Ratspräsidentschaft
- **16.Januar 2023:**
  - Verordnung in Kraft gesetzt
- **Bis Juli 2024:**
  - Weitere Spezifikationen durch regulatorische technische Standards (RTS)
- **17.01.2025:**
  - Anwendung der Verordnung
- **Anfang 2025:**
  - Voraussichtlicher Beginn der Überwachung durch die Behörden

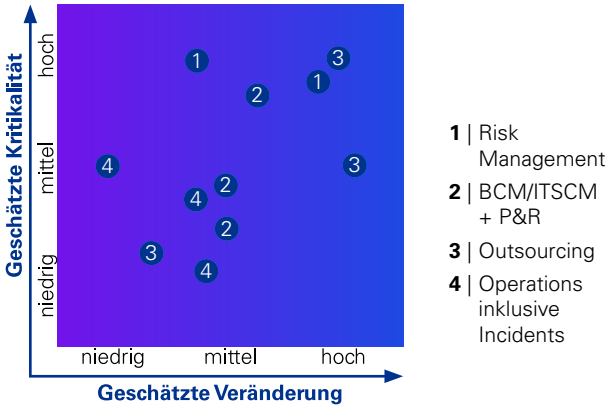
Quelle: KPMG in Deutschland, 2023

DORA stellt Banken und Versicherer vor neue Aufgaben zur Sicherstellung Ihrer operativen Resilienz…



Quelle: KPMG in Deutschland, 2023

...daraus lassen sich folgende zentrale Handlungsfelder[2] identifizieren



Quelle: KPMG in Deutschland, 2023

DORA ist keine reine Compliance-Anforderung. Durch die Vereinheitlichung der Regulierung bietet DORA Finanzinstituten die Möglichkeit, operative Risikokontrollkapazitäten zu bündeln. Gleichzeitig wird ein hohes Maß an operativer Bereitschaft und Widerstandsfähigkeit in der gesamten Organisation erreicht.

Durch unsere Projekterfahrung gehen wir von folgenden Änderungsbedarfen bei der Einführung der DORA aus.

[1] xAIT: BAIT, VAIT
[2] Grundlage aktuelle VAIT-Anforderungen

Lernen Sie Ihren DORA-Ist-Stand mit unserem KPMG-Ansatz kennen

01 Scoping relevanter Organisationseinheiten und Projektplanung mithilfe von vorhandenen xAIT/ ISO/NIST Mapping und Interpretation der DORA

02 Toolbasierte Gap-Analyse auf Grundlage von ausgewählten Kerndokumenten und Interviews

03 Konsultation der vorläufigen Ergebnisse mit den fachlichen Ansprechpersonen

04 Präsentation der Ergebnisse der Gap-Analyse inklusive Heatmap zur Priorisierung

05 Definition eines ganzheitlichen Maßnahmenplans (inklusive. Integration mit bestehenden Maßnahmen) zur Behebung der identifizierten Gaps

Risikobasierter Realitäts-Check (Implementierungsstatus) + **Umsetzungs-Support**

Die Anforderungen der Verordnung über die digitale operationelle Resilienz gehen über die Anforderungen schon bestehender Regulationen hinaus. Einige zusätzliche Anforderungen werden im Folgenden hervorgehoben:

ICT Risk Management Framework
- Wichtige Rolle des Leistungsorgans
- Anforderung einer Strategie für digitale Resilienz

Testen der digitalen operationalen Resilienz
- Programm zum Testen der Widerstandsfähigkeit des digitalen Geschäftsbetriebs
- Bedrohungsbasierte Penetrationstests

IKT-bezogene Vorfälle
- Mechanismen zur Erkennung ungewöhnlicher Aktivitäten
- Krisenmanagementfunktion
- Unabhängige Prüfung von Wiederherstellungsplänen

Managing des IKT-Drittparteienrisikos
- Strategie zur Nutzung mehrerer IKT-Anbieter
- Strategie für IKT-Risiken von Drittdienstleister
- Ausstiegstrategienstrategien
- Prozessdokumentation von IKT-Drittdienstleistern

Gerne unterstützt Sie unser Team

KPMG AG Wirtschaftsprüfungsgesellschaft
Klingelhöferstraße 18
10785 Berlin

Vaike Metzger
Partnerin, Financial Services
M +49 172 2895793
vmetzger@kpmg.com

Julian Dersch
Manager, Financial Services
M +49 151 42566204
jdersch@kpmg.com

Nicolas Täuber
Manager, Financial Services
M +49 151 72751209
ntaeuber@kpmg.com

Einige oder alle der hier beschriebenen Leistungen sind möglicherweise für KPMG Prüfungsmandanten und deren verbundene Unternehmen unzulässig.

www.kpmg.de
www.kpmg.de/socialmedia

Die enthaltenen Informationen sind allgemeiner Natur und nicht auf die spezielle Situation einer Einzelperson oder einer juristischen Person ausgerichtet. Obwohl wir uns bemühen, zuverlässige und aktuelle Informationen zu liefern, können wir nicht garantieren, dass diese Informationen so zutreffend sind wie zum Zeitpunkt ihres Eingangs oder dass sie auch in Zukunft so zutreffend sein werden. Niemand sollte aufgrund dieser Informationen handeln ohne geeigneten fachlichen Rat und ohne gründliche Analyse der betreffenden Situation.

© 2023 KPMG AG Wirtschaftsprüfungsgesellschaft, eine Aktiengesellschaft nach deutschem Recht und ein Mitglied der globalen KPMG-Organisation unabhängiger Mitgliedsfirmen, die KPMG International Limited, einer Private English Company Limited by Guarantee, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind Marken, die die unabhängigen Mitgliedsfirmen der globalen KPMG-Organisation unter Lizenz verwenden.