Trust and Technology Blog

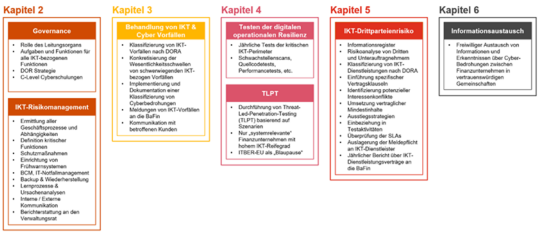
By PwC Deutschland | 08. Juli 2024

# Die BaFin wird konkret - Umsetzungshinweise für den Digital Operational Resilience Act (DORA)

**Mit dem Inkrafttreten des Digital Operational Resilience Act (DORA) am 16. Januar 2023 und der bevorstehenden Anwendungsfrist ab dem 17. Januar 2025 stehen Finanzunternehmen vor der Herausforderung, ihre IT-Systeme und Prozesse den neuen europäischen Vorgaben anzupassen.**

Mit dem Inkrafttreten des Digital Operational Resilience Act (DORA) am 16. Januar 2023 und der bevorstehenden Anwendungsfrist ab dem 17. Januar 2025 stehen Finanzunternehmen vor der Herausforderung, ihre IT-Systeme und Prozesse den neuen europäischen Vorgaben anzupassen. DORA zielt darauf ab, die digitale operationale Resilienz im Finanzsektor zu stärken und ein einheitliches Regelwerk für den Umgang mit IKT-Risiken und Cybersicherheit zu schaffen.

Die BaFin hat in Zusammenarbeit mit der Deutschen Bundesbank und Vertretern der Finanzindustrie Umsetzungshinweise erarbeitet, die Finanzunternehmen bei der Implementierung der DORA-Anforderungen unterstützen sollen.
Dieser Artikel fasst die zentralen Punkte der Umsetzungshinweise zusammen und bietet Ihnen einen Überblick über die Herausforderungen bei der Implementierung von DORA.




Die Umsetzungshinweise gliedern sich in verschiedene Bereiche, darunter Governance und Organisation, Informationsrisiko- und Informationssicherheitsmanagement, IT-Betrieb, IKT-Geschäftsfortführungsmanagement, IT-Projektmanagement und Anwendungsentwicklung, IKT-Drittparteienrisikomanagement, operative Informationssicherheit sowie Identitäts- und Rechtemanagement. In den Umsetzungshinweisen wurde der IKT-Risikomanagementrahmen und das IKT-Drittparteirisikomanagement sowie die bereits veröffentlichten dazugehörigen RTS-/ ITS-Entwürfe den Anforderungen der BAIT und VAIT gegenübergestellt.

Eine wesentliche Neuerung ist die Einführung einer IKT-Geschäftsfortführungsleitlinie, die als Teil der allgemeinen Geschäftsfortführungsleitlinie die Reaktion auf IKT-bezogene Vorfälle, die Aktivierung von Eindämmungsmaßnahmen und die Einschätzung von Auswirkungen, Schäden und Verlusten regelt. Diese Leitlinie basiert auf den Identifizierungsanforderungen des Art. 8 DORA und ist in den bisherigen regulatorischen Anforderungen der xAIT in dieser Form nicht vorhanden.

Ein zentraler Aspekt ist die Erweiterung der zu berücksichtigenden Szenarien im Rahmen des Notfallmanagements. Finanzunternehmen sind nun verpflichtet, auch die Auswirkungen des Klimawandels, Insider-Angriffe, politische und soziale Instabilität sowie großflächige Stromausfälle in ihre Notfallkonzeption einzubeziehen.

Des Weiteren sind die IKT-Geschäftsfortführungspläne nun mindestens jährlich zu testen.

Ein weiterer Schwerpunkt liegt auf der Betriebsstabilität und der Aktualisierung von IKT-Systemen. DORA fordert, dass diese Systeme stets auf dem neuesten Stand gehalten werden und auch in angespannten Marktphasen eine angemessene Informationsverarbeitung gewährleisten. Dies geht über die bisherige

Regulierung hinaus, welche primär Aktualisierungen der IT-Systeme verlangte.

Die Definition von vertraglichen Vereinbarungen zur Nutzung von IKT-Dienstleistungen wurde im Vergleich zu den bisherigen Auslagerungsdefinitionen deutlich erweitert. Insbesondere bezieht sich diese für Finanzunternehmen auf alle "IKT-Dienstleistungen für die Ausübung ihrer Geschäftstätigkeit". Dies erfordert eine noch umfassendere Bewertung aller Drittanbieterbeziehungen mit IKT-Bezug.
Mit DORA wird außerdem eine IKT-Risikokontrollfunktion eingeführt, welche die Zuständigkeit für das Management und die Überwachung des IKT-Risikos übernehmen soll. Diese Funktion ähnelt dem Informationssicherheitsbeauftragten (ISB), kann allerdings aufgrund des Fokus auf das IKT-Risiko nicht mit dem ISB gleichgestellt werden.

Wichtig zu beachten ist dennoch, dass trotz des Wegfalls der xAIT (BAIT, VAIT, etc.), die Inhalte der xAIT eine wesentliche Grundlage für die Erfüllung der DORA-Compliance bilden und deshalb nicht vergessen werden dürfen. DORA legt zwar, im Vergleich zur bisherigen Regulatorik einen stärkeren Fokus auf das IKT-Risikomanagement, jedoch baut genau dieses auf der aktuell (noch) geltenden Regulatorik auf.

Haben Sie Fragen zu diesen regulatorischen Änderungen oder benötigen Sie Unterstützung bei der Umsetzung? Unser Team steht Ihnen gerne mit Fachwissen und einen erprobten Toolset beratend zur Seite!

Laufende Updates zum Thema erhalten Sie über das regulatorische Horizon Scanning in unserer Recherche-Applikation PwC Plus. Lesen Sie hier mehr über die Möglichkeiten und Angebote.

Zu weiteren PwC Blogs

**Schlagwörter**

Artificial Intelligence (AI), Digital Operational Resilience Act (DORA), Digitalisierung, Finanzmarkt, IT-Sicherheit, IT-Systeme, Informationstechnologie (IT)

**Kontakt**

**Rüdiger Giebichenstein**

Köln

ruediger.giebichenstein@pwc.com