

CIO Advisory

DORA in Finanzunternehmen

Operationale Resilienz & Compliance



DORA im Zeitablauf

Die EU-Verordnung DORA (Digital Operational Resilience Act) beinhaltet einheitliche Vorgaben zur Gewährleistung der digitalen Betriebsstabilität für die einzelnen betroffenen Finanzunternehmen. Sie zielt damit, unter Wahrung der Innovations- und Wettbewerbspotenziale, auf die Verbesserung der Resilienz des gesamten Finanzsektors in der EU ab.

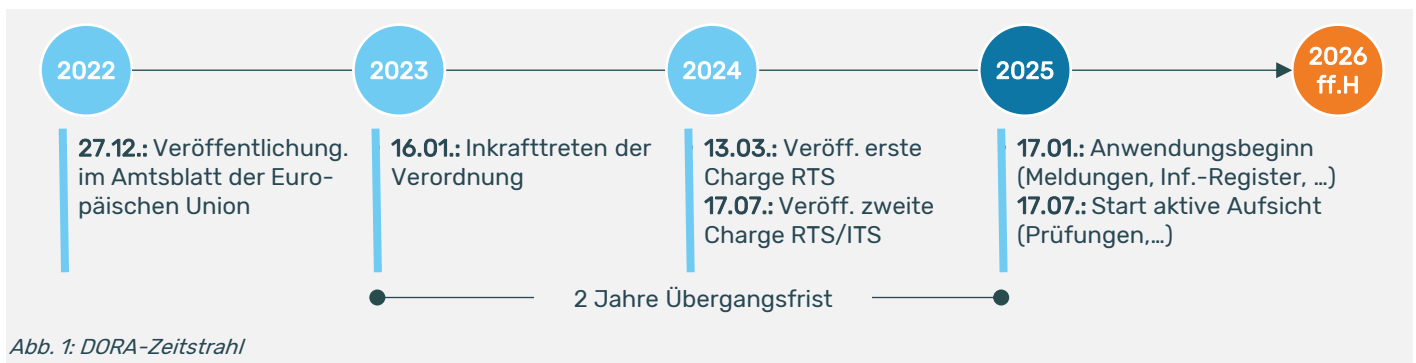
Zugrunde liegt dabei die Erkenntnis, dass die Nutzung von Informations- und Kommunikationstechnologie (IKT) neben deren Chancen auch viele Risiken für die Finanzunternehmen beinhaltet. Mit der Nutzung entstehen hohe Abhängigkeiten sowohl von IKT als auch von Drittdienstleistern, welche diese für den Geschäftsbetrieb der Unternehmen bereitstellen. Die parallel dazu steigende (Cyber)Bedrohungslage erhöht das Risiko des Ausfalls von vitalen Geschäftsprozessen ganzer Finanzunternehmen oder wichtiger Finanzdienstleistungsketten.

DORA umfasst daher die Themen IKT-Risikomanagement, IKT-bezogene Vorfälle, Resilienztests und IKT-Drittparteienrisiko. Die Themen bilden einen harmonisierten, verbindlichen Rahmen zur Verbesserung der digitalen Resilienz.

Dieser Rahmen erfordert bei den Finanzunternehmen, sich die Bedrohungen und Risiken zu vergegenwärtigen, sich damit auseinanderzusetzen und angemessen zu steuern. Kritisch dabei ist die Erkenntnis, dass aus den Vorgaben ableitbare Maßnahmen nicht nur einer nachweislichen DORA-Compliance dienen. Vielmehr gewährleistet ihre Wirksamkeit den Bestand und Erfolg des Kerngeschäfts.

DORA ist etabliert

Seit der Veröffentlichung der DORA-Verordnung im Amtsblatt der EU Ende 2022 wurden auch die ergänzenden RTS/ITS¹ und Guidelines sukzessive veröffentlicht. Damit liegen alle umzusetzenden Vorgaben für den Kreis der betroffenen Finanzunternehmen vor. Flankiert werden sie von aufsichtlichen Mitteilungen zur Sensibilisierung, Klarstellung und Unterstützung. Seit etwa Mitte 2025 umfassen aufsichtliche Prüfungen DORA-Inhalte.



Erkenntnisse aus den Jahren bis 2025

Die vergangenen Jahre waren seit der DORA-Veröffentlichung vorwiegend von Analyse- und Umsetzungsprojekten geprägt. Dabei traten wesentliche inhaltliche Themen und Aufwandstreiber zutage. Exemplarisch übergreifend können genannt werden:

Compliance zu xAIT – Gute Basis

Die bisherigen aufsichtl. Anforderungen an die IT sind (inhaltlich) nicht obsolet. Sie wirken, wenn vorhanden, als „Umsetzungsbeschleuniger“. So bildet z. B. ein funktionierender Informationsverbund unverändert eine gute Grundlage für viele DORA-Anforderungen.

Fristen und Termine – Planbestimmend

Vorgaben wie z. B. die IKT-Vorfalldmeldung oder die Meldung des Informationsregisters sind mit engen Fristen und Terminen versehen. Deren Einhaltung war ein bestimmender Faktor in der Planung und Umsetzung der erforderlichen Maßnahmen.

Kritische oder wichtige Funktionen (KowF) – Key

Eine tragfähige Definition und Identifikation der KowF ist eine sehr wichtige Basis. Denn sie wirkt z. B. unmittelbar auf das IKT-Vorfalldmanagement, das IKT-Drittdienstleistermanagement, das Testing oder das Identity- und Accessmanagement (PAM).

IKT-Drittparteienmgmt. – Aufwandstreiber

Die Datenlage bei Auslagerungen/Ausgliederungen stellt eine große Herausforderung im Kontext von z. B. Informationsregister oder Vertragsbestandteilen dar. Die Aufwände fallen auch nach einer Erstumsetzung langfristig an.

¹ RTS - Regulatory Technical Standards; ITS - Implementing Technical Standards



Womit sind Finanzunternehmen jetzt konfrontiert?

Die Finanzunternehmen befinden sich in verschiedenen Phasen ihrer individuellen „Road to Resilience & Compliance“. Zum aktuellen Zeitpunkt begegnen uns hier **3 typische Ausgangslagen**. Unternehmen, die in der DORA-Umsetzung bereits fortgeschritten sind und nun die Wirksamkeit und Effizienz in den Fokus nehmen. Unternehmen, die perspektivisch vor einer Prüfung stehen oder sich zeitig darauf vorbereiten möchten. Und jene, die über das Finanzmarktdigitalisierungsgesetz (FinmadiG) mit DORA-Anforderungen neu konfrontiert sind.

| 1 Operationalisierungs-/ Optimierungsbedarf | 2 Bevorstehende DORA-Prüfung | 3 Neu betroffen (via FinmadiG) |
|--|--|---|
| <ul style="list-style-type: none"> • Wie kann ich die Wirksamkeit der DORA-Vorgaben operativ herstellen/erhöhen? • Welche Maßnahmen kann ich ergreifen, um die Organisation/Ressourcen zu entlasten? | <ul style="list-style-type: none"> • Wie läuft eine DORA-Prüfung ab und welche Erkenntnisse gibt es aus bisherigen Prüfergebnissen? • Wie kann ich mich organisatorisch bestmöglich auf die Prüfung vorbereiten? | <ul style="list-style-type: none"> • Wie ist mein aktueller Stand hinsichtlich der DORA-Vorgaben? • Welche Vorgaben sollte ich priorisiert umsetzen und mit welchen „good practices“? |

Abb. 2: Typische Ausgangslagen der Finanzunternehmen und Fragestellungen

Operationalisierung und Optimierungen – Umsetzung V1.1

In vielen Finanzunternehmen wurden bereits DORA-Programme/-projekte durchgeführt oder befinden sich noch in der Umsetzung. Die Aktivitäten zielten oft zunächst auf die Einhaltung von Fristen (z. B. IKT-Vorfallmeldung, Informationsregister) oder die Verankerung der DORA-Vorgaben in internen Anweisungen ab.

Damit ist eine gute Basis gelegt, es gibt aber noch **Handlungsfelder**. Die operative Umsetzung läuft oft nicht reibungslos oder fehlt in Teilen noch. Somit ist in vielen Finanzunternehmen bisher nur eine eingeschränkte Wirksamkeit vorhanden. Auch sind diese ersten Lösungen operativ oft noch mit fehleranfälligen Tools (z. B. Excel) umgesetzt oder prozessual mit hohem Arbeitsaufwand behaftet.

Es besteht der Bedarf, **Wirksamkeitslücken zu schließen** und zu prüfen, wo **Abläufe effizienter gestaltet** werden können.

Aufsichtliche Prüfungen – Veränderte Prüfungspraxis

Seit etwa Mitte 2025 prüft die Aufsicht die Umsetzung von DORA mit den RTS/ITS in den Finanzunternehmen. Die aufsichtlichen Prüfungen sind dabei in insgesamt **10 Prüffelder** strukturiert. Dabei sind nicht immer alle Prüffelder Gegenstand und werden, abhängig vom z. B. Geschäftsmodell, in unterschiedlicher Tiefe beleuchtet.

Prüfergebnisse die plenum aus der Praxis vorliegen, verzeichnen eine hohe Anzahl zum Teil schwergewichtiger Mängel, insbesondere im IKT-Risikomanagementrahmen. Der Bereich IKT-Drittparteiensrisikomanagement wurde im Transformationsjahr 2025 dagegen noch nicht tiefgehend geprüft. Die BaFin und Bundesbank haben jedoch angekündigt, ab 2026 eine vollständige Umsetzung in allen Prüffeldern vorauszusetzen.

Als Erkenntnis daraus ist es empfehlenswert, den Prüfteams durch eine gute **Prüfungsvorbereitung** zu begegnen und von bisherigen **Erkenntnissen aus dem Prüfungsablauf und festgestellten Mängel** zu profitieren.

Neue Betroffene – Start mit Erleichterungen

Durch das Finanzmarktdigitalisierungsgesetz (FinmadiG) unterliegen weitere Finanzunternehmen dem Anwendungsbereich von DORA und den flankierenden RTS/ITS. Zum Kreis der neu Betroffenen gehören z. B. Bürgschaftsbanken, Finanzierungsleasing- und Factoringunternehmen, Kryptowertpapierregisterführer, Wohnungsunternehmen mit Spareinrichtung oder Drittstaaten-zweigstellen nach § 53 KWG.

Für diese Finanzunternehmen gibt es einige **Erleichterungen (entfallende Inhalte)**, wie z. B. die Anwendung eines **vereinfachten IKT-Risikomanagementrahmens**. Jedoch verbleiben auch im IKT-Risikomanagement sowie insbesondere im IKT-Drittparteiensrisikomanagement und der IKT-Geschäftsfortführung erhebliche neue Anforderungen gegenüber den bisherigen xAIT.

Die Zeit bis zur **gesetzten Umsetzungsfrist am 01.01.2027** ist daher gut zu nutzen, um ein verbessertes Resilienz-Niveau und die geforderte Compliance zu erreichen.



plenum DORA-Leistungsportfolio

Jede Phase der „Road to Resilience & Compliance“ hat ihre eigenen Herausforderungen und Zielsetzungen. Von der Standortbestimmung und Awareness zu Beginn, über die erfolgreiche Erreichung der Compliance unter der Überwachung der aufsichtlichen Prüfer, bis hin zu Erkenntnissen darüber, ob die Maßnahmen auch optimal greifen.

Insbesondere Optimierungen und Resilienz-Checks sind Voraussetzungen dafür, dass Sie die Früchte ihrer Anstrengungen, z. B. schnellere Reaktion und Wiederherstellung oder hohes Vertrauen der Kunden auch ernten können und diese einen Beitrag zum Geschäftserfolg leisten.



Analyse & Standortbestimmung

Mittels einer strukturierten und vielfach bewährten Gap-Analyse identifizieren wir mit Ihnen die Lücken zwischen den DORA-Anforderungen (inkl. RTS/ITS) und dem Status Quo Ihres Unternehmens.

Planung & operative Umsetzung

Aufbauend auf z. B. der Gap-Analyse oder den Feststellungen der Aufsicht definieren und planen wir mit Ihnen Maßnahmen sowie Schulungen und setzen diese operativ in der Organisation um.

Optimierung & Tooleinsatz

Wir identifizieren Potenziale in aktuellen Implementierungen und erarbeiten Verbesserungsmöglichkeiten wie z. B. Tools zum Informationsregister oder die Integration von Aktivitäten in Workflow-Systeme.

Prüfungsvorbereitung & -begleitung

Im Vorfeld einer aufsichtlichen Prüfung stellen wir mit Ihnen die organisatorische und fachliche Readiness auf Basis von „Good Practices“ her und begleiten Sie in der Prüfungsorganisation durch den Ablauf.

Funktionsübernahme as a Service

Wir stellen erfahrene Mitarbeiter für Funktionsübernahmen der z. B. IKT-Risikomanagementfunktion oder eines IKT-Drittparteimanagers (as a Service) zur Ressourcenentlastung oder zum Know-How-Aufbau.

Resilienz- & Wirksamkeits-Checks

Wir prüfen, wie wirksam und nachhaltig die implementierten Maßnahmen zur Resilienz sind, z. B. durch Notfall-Tests oder den Einsatz unseres Offensive Security Teams im Pentesting und Red-Teaming.

Resilienz steigern und Regulatorik wirksam umsetzen – mit plenum

plenum hat eine Vielzahl von Finanzunternehmen bei der kundenspezifischen Strukturierung, Planung und Umsetzung der DORA-Anforderungen unterstützt. Mit unserem praxisbewährten Vorgehen bieten wir Ihnen eine verlässliche und pragmatische Begleitung in jeder Phase Ihrer „Road to Resilience & Compliance“.