

Blog Post

N° 1/2025

# DORA – Status Quo 2025

*Von der Regulierungsidee zur Umsetzung in der Praxis*

Dr. Andreas Windisch

**ASQUARED**

asquared Blog Post N° 1/2025

September 2025

Copyright © asquared GmbH

Seit Januar 2025 ist der Digital Operational Resilience Act (DORA) verbindlich. Banken, Versicherer, Zahlungsdienstleister und FinTechs müssen zeigen, dass sie widerstandsfähig gegen IT-Störungen und Cyberangriffe sind. Während große Player Fortschritte machen, kämpfen viele kleinere Institute noch mit praktischen Hürden. Wo stehen wir? Was sind die Herausforderungen? Wie lauten konkrete Handlungsempfehlungen?

## DORA im Jahr 2025

Im September 2020 berichteten wir über den Verordnungsvorschlag der EU-Kommission zur digitalen operativen Resilienz im Finanzsektor – kurz DORA. Heute, fünf Jahre später ist die Verordnung Realität, die Übergangsfristen sind abgelaufen und die Unternehmen müssen sich im Alltag mit den Anforderungen auseinandersetzen. Die folgende Abbildung zeigt die maßgeblichen Meilensteine von der Veröffentlichung des Entwurfs bis hin zu den aktuellen und kommenden Umsetzungspflichten.

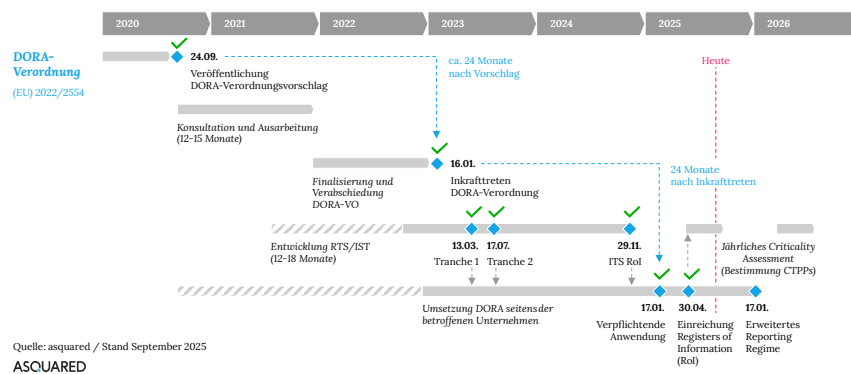


Abbildung 1: Konkretisierte DORA-Timeline (Stand September 2025)

Seit dem 17. Januar 2025 gelten die Umsetzungspflichten für alle betroffenen Finanzunternehmen verbindlich. Mit den erweiterten Incident-Reporting-Pflichten ab Januar 2026 rücken weitere regulatorische Anforderungen unmittelbar näher. Doch wo stehen wir heute in der praktischen Umsetzung?

## Aktueller Stand der DORA-Umsetzung in der Praxis

Mehr als sechs Monate nach dem Stichtag zur verpflichtenden Anwendung zeichnet sich ein deutlich differenziertes Bild. Große Banken und Versicherungen konnten vielfach auf bereits bestehende regulatorische Rahmenwerke wie BAIT, VAIT oder EBA-Guidelines aufbauen. Sie haben ihre Governance-Strukturen erweitert, Verantwortlichkeiten auf Vorstandsebene klar definiert und Prozesse für Incident Reporting sowie IT-

Risikomanagement formalisiert. Bei ihnen ist DORA heute meist ein Thema, das in den regulären Aufsichtsm Meetings des Managements verankert ist.

Mittlere Finanzdienstleister, Zahlungsinstitute und Wertpapierfirmen befinden sich hingegen in einer intensiven Transformationsphase. Viele haben zwar Projektstrukturen eingerichtet, kämpfen jedoch noch mit der vollständigen Integration von Monitoring-Tools, der Implementierung von automatisierten Vorfallmeldungen und der Anpassung ihrer Outsourcing-Verträge. Oft sind noch Übergangslösungen im Einsatz, bei denen Vorfälle zwar erkannt, aber nicht in der von DORA geforderten Geschwindigkeit und Qualität gemeldet werden.

Kleinere Institute und FinTechs sehen sich mit der Herausforderung konfrontiert, dass DORA-Compliance in keinem Verhältnis zu ihren bisherigen Ressourcen steht. Fachpersonal für Cyber- und Resilienzthemen ist knapp, interne Kompetenzen fehlen häufig. Die Folge: Viele kleinere Marktteilnehmer arbeiten mit externen Beratern oder Dienstleistern, um zumindest die grundlegenden Anforderungen wie Risikoinventarisierung und Dokumentation abdecken zu können.

Branchenübergreifend gilt: Nur ein Bruchteil (ca. 4 %) der Institute gibt an, DORA vollständig als Business-as-Usual integriert zu haben. Für die meisten Unternehmen bleibt DORA ein laufendes Umsetzungsprogramm, das neben dem operativen Geschäft weitergeführt werden muss.

## **Praktische Herausforderungen in der Umsetzung**

Die Anforderungen von DORA sind weitreichend und berühren alle Bereiche der Finanzwirtschaft. In der Praxis kristallisieren sich fünf typische Problemfelder heraus:

### **1 Banken – Incident Reporting in Echtzeit**

Banken müssen schwerwiegende IKT-Vorfälle innerhalb enger Fristen an die Aufsicht melden. Die Realität: Viele internationale Institute betreiben noch heterogene IT-Landschaften mit unterschiedlichen Logging- und Meldesystemen. Im Frühjahr 2025 zeigte ein Cyberangriff auf eine große europäische Bank, dass interne Eskalationswege nicht synchronisiert waren – dadurch konnte die Erstmeldung an die Aufsicht nur mit Verzögerung erfolgen. Laut einer Analyse von CeF-Pro (Mai 2025) kämpfen 43 % der Institute mit der termingerechten Umsetzung von Incident Reporting, besonders im Zusammenhang mit der Harmonisierung interner Prozesse.

### **2 Versicherungen – Resilienztests unter Realbedingungen**

Versicherungen sind verpflichtet, regelmäßig umfassende Resilienztests durchzuführen, darunter Threat-Led Penetration Tests (TLPT). In der Praxis scheitert

es oft an der Komplexität: Bei einem Rückversicherer ergab ein Test, dass Backup-Systeme zwar vorhanden, aber nicht ausreichend voneinander getrennt waren. Der simulierte Angriff konnte dadurch auch die Redundanzsysteme kompromittieren – ein Szenario, das im Ernstfall den Geschäftsbetrieb lahmgelegt hätte. Eine Übersicht über die Herausforderungen bei der DORA-Umsetzung zeigt ein Bericht von Insurance Europe (Januar 2025): Vollständige Compliance war trotz bestehender Praktiken weiterhin eine große Herausforderung.

### 3 **Zahlungsdienstleister – Drittanbieterabhängigkeit**

Payment Provider sind stark von Cloud-Diensten abhängig. Ein mittelgroßes Institut stellte im Frühjahr 2025 fest, dass Verträge mit einem US-amerikanischen Cloud-Anbieter weder Audit-Rechte noch Exit-Strategien im Sinne von DORA vorsahen. Dies führte zu teuren Nachverhandlungen, die parallel zum operativen Geschäft erhebliche Ressourcen banden. Laut Pillsbury (Juli 2025) konnten viele Finanzunternehmen ihre Register of Information und Vertragsanpassungen erst nach dem Inkrafttreten der DORA abschließen – insbesondere bei Drittanbieterverträgen.

### 4 **Asset Manager – Datenklassifizierung und -schutz**

DORA fordert eine präzise Inventarisierung und den Schutz kritischer Daten. Viele Asset Manager tun sich schwer mit der Konsolidierung historisch gewachsener Datenbestände. Ein Fall zeigte, dass Kundendaten über Jahre in unterschiedlichen Legacy-Systemen ohne Notfallpläne gespeichert waren. Die fehlende Transparenz über Datenflüsse stellte ein erhebliches Compliance-Risiko dar. Numerix (Februar 2025) beschreibt, dass Organisationen häufig Schwierigkeiten haben, Daten zu konsolidieren und Due-Diligence-Vorgaben zu DORA-konformen Drittanbietern umzusetzen.

### 5 **FinTechs – Ressourcen und Fachwissen**

Start-ups und junge FinTechs agieren oft agil, haben aber keine etablierten Governance-Strukturen. Ein Berliner FinTech mit 120 Mitarbeitern musste feststellen, dass es keine formalen Prozesse für Incident Response gab. Erst durch externe Berater wurden Grundlagendokumentationen erstellt und Schulungen organisiert. Hier zeigt sich: Für kleine, dynamische Player ist DORA ein kultureller und organisatorischer Kraftakt. SANS (Mai 2025) warnen: „If you haven't started implementing measures yet, you're already late“ – viele kleinere Anbieter fehlen interne Strukturen und Know-how zur DORA-Umsetzung.

## **Konkrete Handlungsempfehlungen**

Um die beschriebenen Herausforderungen zu meistern, müssen Unternehmen aktiv(er) werden. Dabei kristallisieren sich mehrere Handlungsfelder heraus, insbesondere:

### 1 **Governance und Verantwortlichkeit stärken**

Aufsichtsbehörden erwarten, dass das Top-Management Verantwortung für die digitale Resilienz übernimmt. Unternehmen sollten daher DORA-Themen fest in ihre Vorstandsagenda integrieren, ein Chief Resilience Officer- oder CISO-Mandat stärken und regelmäßige Schulungen für Führungskräfte durchführen.

- Board-Trainings zu Cyber- und Resilienzthemen einführen: Regelmäßige Awareness-Sessions für Vorstände, z. B. nach dem NIST Cybersecurity Framework strukturiert.
- Einführung eines Chief Resilience Officer (CRO) oder Stärkung des CISO: Mandat mit klarer Reporting-Linie zum Vorstand; etabliert Accountability im Sinne von Art. 5 DORA.
- Reifegradanalysen mit COBIT oder ISO 27001: Benchmarking gegen internationale Standards zur Identifikation von Governance-Lücken.

### 2 **Automatisierte Incident-Response-Systeme einführen**

Manuelle Prozesse reichen nicht mehr aus. Der Einsatz von Security Information and Event Management (SIEM)-Systemen, SOAR-Plattformen und automatisierten Reporting-Tools ist entscheidend, um Vorfälle in der von DORA geforderten Geschwindigkeit zu erkennen, zu klassifizieren und zu melden.

- Einführung eines SIEM-Systems (z. B. Splunk, IBM QRadar, Azure Sentinel), um Logdaten zentral zu sammeln und Echtzeit-Korrelationen aufzubauen.
- SOAR-Plattform nutzen (z. B. Palo Alto Cortex XSOAR), um Playbooks für automatisierte Reaktionen zu erstellen – z. B. automatisches Blockieren kompromittierter Accounts.
- Regelmäßige Red-Team-/Blue-Team-Übungen nach MITRE ATT&CK-Methodik, um Incident-Response-Pläne realistisch zu testen.

### 3 **Vertragsmanagement professionalisieren**

Outsourcing- und Cloud-Verträge sollten systematisch überprüft und auf DORA-konforme Standardklauseln angepasst werden. Dazu gehören Audit-Rechte, Sub-Outsourcing-Regelungen und klare Exit-Strategien. Viele Unternehmen bauen zentrale Contract-Management-Units auf, die regulatorische Anforderungen in die Vertragsgestaltung einfließen lassen.

- Einrichtung eines zentralen Outsourcing-Registers nach DORA-Vorgaben; Tools wie ServiceNow Vendor Risk Management oder Archer unterstützen die Übersicht.
- Standardvertragsklauseln nach EBA Outsourcing Guidelines: Audit-Rechte, Sub-Outsourcing-Approval, Exit-Strategien klar regeln.

- Durchführung von Supplier Audits nach ISO 27036 (IT-Supplier Management), um die Sicherheit der Dienstleister regelmäßig zu prüfen.

#### 4 **Resilienztests und Notfallübungen intensivieren**

DORA fordert nicht nur Tests, sondern auch eine klare Ableitung von Lessons Learned. Unternehmen sollten regelmäßige Krisensimulationen durchführen – inklusive Teilnahme von Vorstand und operativen Teams. Nur so lassen sich Schwachstellen realitätsnah identifizieren.

- Durchführung von Threat-Led Penetration Tests (TLPT) nach dem TIBER-EU-Framework, um Angriffe unter Realbedingungen zu simulieren.
- Business Continuity Management (BCM) mit ISO 22301: Planung und Test von Wiederanlauf-Szenarien, inkl. Failover in Backup-Rechenzentren.
- Tabletop Exercises für Vorstände: Szenario-Workshops, bei denen die Geschäftsführung durch simulierte Krisen geleitet wird.

#### 5 **Kooperationen und Wissensaustausch fördern**

Cyber-Bedrohungen machen nicht an Unternehmensgrenzen halt. Brancheninitiativen wie Financial ISACs oder nationale CERTs bieten Plattformen, um Bedrohungsinformationen auszutauschen. Unternehmen sollten aktiv teilnehmen, um von Frühwarnungen zu profitieren und eigene Resilienzstrategien zu schärfen.

- Teilnahme an branchenspezifischen ISACs (Information Sharing and Analysis Centers), z. B. FS-ISAC für Finanzunternehmen.
- Etablierung interner Threat-Intelligence-Funktion: Nutzung von Plattformen wie MISP (Malware Information Sharing Platform) oder ThreatConnect.
- Regelmäßige Teilnahme an CERT-Trainings (z. B. bei nationalen Computer Emergency Response Teams), um Frühwarnungen und Handlungsempfehlungen zu integrieren.

## Fazit

Fünf Jahre nach der Veröffentlichung des Entwurfs ist DORA Realität. Während große Akteure im Finanzsektor ihre Strukturen angepasst haben, stehen viele insbesondere kleinere Unternehmen noch vor erheblichen Herausforderungen. DORA ist kein abgeschlossenes Projekt, sondern ein laufender Anpassungsprozess. Das bedeutet, jetzt gezielt in konkrete Maßnahmen zu investieren: Incident-Response-Prozesse automatisieren, Outsourcing-Verträge überarbeiten, Resilienztests in den Regelbetrieb integrieren und Governance-Strukturen auf Vorstandsebene stärken. Ebenso wichtig ist der Aufbau einer Kultur der Zusammenarbeit – etwa durch den aktiven Austausch in Cyber-Threat-Intelligence-Netzwerken. Wer diese Schritte priorisiert, schafft nicht nur Compliance, sondern baut nachhaltige digitale Resilienz auf.

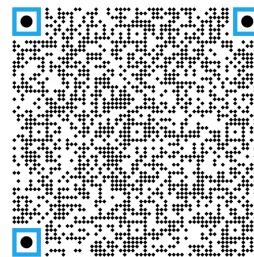
## Quellenangaben

- 1 TechRadar, „DORA: six months into a resilience revolution“, <https://www.techradar.com/pro/dora-six-months-into-a-resilience-revolution>
- 2 TechRadar, „Regulatory compliance: Act now“, <https://www.techradar.com/pro/regulatory-compliance-act-now>
- 3 PwC Luxembourg, „DORA: laying the groundwork“, <https://www.pwc.lu/en/press/press-releases-2025/dora-laying-the-groundwork.html>
- 4 Help Net Security, „DORA compliance challenges for financial firms“, <https://www.helpnetsecurity.com/2025/07/25/dora-compliance-challenges-financial-firms>
- 5 Bird & Bird, „How well is Europe’s financial sector prepared for DORA?“, <https://www.twobirds.com/en/insights/2025/global/how-well-is-europes-financial-sector-and-its-it-supply-chains-prepared-for-dora>
- 6 CeFPro, „Most banks still not ready for DORA“, <https://connect.cefpro.com/article/view/most-banks-still-not-ready-for-dora>
- 7 Insurance Europe, „Strengthening the industry’s cyber resilience: Insights into the implementation of the Digital Operational Resilience Act“, <https://insuranceeurope.eu/news/3275/strengthening-the-industry-s-cyber-resilience-insights-into-the-implementation-of-the-digital-operational-resilience-act>
- 8 Pillsbury, „DORA: EU Financial Entities and Service Providers Face New Operational Resilience Requirements“, <https://www.pillsburylaw.com/en/news-and-insights/dora-eu-financial-entities-service-providers.html>
- 9 Numerix, „What the DORA Regulation Means for Financial Institutions in 2025“, <https://www.numerix.com/resources/blog/what-dora-regulation-means-financial-institutions-2025>
- 10 SANS Institute, „Navigating DORA & NIS2 Compliance: What EU Financial Sector Organizations Need to Know“, <https://www.sans.org/blog/navigating-dora-nis2-compliance-eu-financial-sector-organisations>

## 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](mailto:contact@asquared.team)

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

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

 [twitter.com/asquaredgmbh](https://twitter.com/asquaredgmbh)

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

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