PPI – Platvoet Performance Intelligence

WHITEPAPER

DORA

Digital Operational Resilience Act

Compliance-Leitfaden für den europäischen Finanzsektor

DORA ist seit dem 17. Januar 2025 verbindlich — und damit kein strategisches Zukunftsthema mehr, sondern eine operative Gegenwartspflicht. Dieses Whitepaper beschreibt die fünf Anforderungssäulen, den betroffenen Adressatenkreis, die Aufsichtsstrukturen und einen praxisorientierten Implementierungspfad für Finanzunternehmen und ihre IKT-Dienstleister.

Autor	Ralf Platvoet, Diplom-Ökonom
Organisation	PPI – Platvoet Performance Intelligence
Stand	Juni 2026 (Verordnungsstand: EU 2022/2554 + RTS/ITS vollständig)
Umfang	ca. 20 Seiten
Themenbereich	Cyber-Compliance · Finanzmarktregulierung · IKT-Risikomanagement

platvoet.org

© 2026 Ralf Platvoet · platvoet.org

Executive Summary

Der Digital Operational Resilience Act (DORA) — Verordnung (EU) 2022/2554 — ist seit dem 17. Januar 2025 vollumfänglich verbindlich anzuwenden. Er schafft erstmals einen EU-weit einheitlichen Rechtsrahmen für die digitale operationale Resilienz im Finanzsektor und löst die fragmentierten nationalen Regelwerke (BAIT, VAIT, KAIT, ZAIT in Deutschland) als primärer Regulierungsrahmen für IKT-Risiken ab.

DORA ist keine technische Spezifikation — es ist ein ganzheitlicher Governance-Rahmen. Er verpflichtet Finanzunternehmen, IKT-Risiken systematisch zu managen, Vorfälle standardisiert zu melden, Resilienztests durchzuführen, Drittanbieter zu überwachen und Informationen mit anderen Marktteilnehmern auszutauschen. Besonders bedeutsam: Das Leitungsorgan — Vorstand und Aufsichtsrat — trägt persönliche Verantwortung für das IKT-Risikomanagement.

Für IKT-Drittdienstleister, die als **Critical Third-Party Providers (CTPPs)** eingestuft werden, gilt darüber hinaus eine direkte Beaufsichtigung durch die europäischen Aufsichtsbehörden (ESAs) — ein regulatorisches Novum mit weitreichenden Implikationen für Cloud-Anbieter, Rechenzentrumsbetreiber und Softwareanbieter im Finanzsektor.

Kernaussagen

- DORA gilt seit 17. Januar 2025 — für Banken, Versicherer, Wertpapierfirmen, Zahlungsinstitute und weitere (ca. 20 Kategorien).
- Für bestimmte kleinere Institute (BAIT-Adressaten) gilt eine Übergangsfrist bis 1. Januar 2027.
- Das Leitungsorgan ist persönlich verantwortlich — Delegation an die IT-Abteilung genügt nicht.
- IKT-Drittanbieter mit kritischer Systemrelevanz werden direkt durch EBA, EIOPA und ESMA beaufsichtigt.
- Erste BaFin-Prüfungen haben begonnen — mit Fokus auf Governance, IKT-Informationsregister und Nachweispflichten.

© 2026 Ralf Platvoet · platvoet.org

1. Kontext: Warum DORA und warum jetzt?

1.1 Das regulatorische Problem vor DORA

Vor DORA regulierten zahlreiche nationale und sektorale Regelwerke das IKT-Risikomanagement im Finanzsektor — fragmentiert, inkonsistent und ohne einheitliche Durchsetzungsmechanismen. In Deutschland galten je nach Institutstyp die BAIT (Banken), VAIT (Versicherer), KAIT (Kapitalverwaltungsgesellschaften) oder ZAIT (Zahlungsdienstleister). Sie alle beruhten auf denselben prinzipienbasierten Grundlagen, aber mit unterschiedlichen Detaillierungsgraden und Prüfpraktiken.

Das Ergebnis: Aufsichtsarbitrage, Lücken bei grenzüberschreitend tätigen Instituten und keine konsolidierte Steuerung systemischer IKT-Risiken auf europäischer Ebene. Besonders kritisch war das fehlende Regulierungsregime für IKT-Drittdienstleister — obwohl ein erheblicher Teil der Finanzinfrastruktur von einer Handvoll globaler Cloud- und Technologieanbieter abhängig ist.

1.2 DORA als Antwort

DORA wurde im September 2020 von der Europäischen Kommission als Teil des Digital Finance Package vorgeschlagen, im November 2022 vom Europäischen Parlament und dem Rat verabschiedet (Verordnung EU 2022/2554) und trat am 16. Januar 2023 in Kraft — mit einer zweijährigen Übergangsfrist zur Implementierung der Regulatory Technical Standards (RTS) und Implementing Technical Standards (ITS).

Das zentrale Versprechen: Ein einheitlicher, EU-weit direkt geltender Standard für digitale operationale Resilienz — ohne nationale Umsetzungsgesetze, ohne Spielräume für Fragmentierung. DORA ist unmittelbar anwendbares EU-Recht in allen Mitgliedstaaten.

Zeitpunkt	Meilenstein
September 2020	Veröffentlichung des Kommissionsentwurfs (Digital Finance Package)
November 2022	Formelle Verabschiedung durch Europäisches Parlament und Rat
16. Januar 2023	Inkrafttreten der Verordnung (EU) 2022/2554
2023–2024	Stufenweise Veröffentlichung der RTS und ITS durch ESAs
17. Januar 2025	Anwendungsbeginn — DORA ist verbindlich für alle Adressaten
März 2025	Erste IKT-Informationsregister an BaFin und andere NCAs zu melden
1. Januar 2027	Übergangsfrist für vereinfachten IKT-Rahmen (BAIT-Adressaten, Kleinstinstitute)

© 2026 Ralf Platvoet · platvoet.org

2. Adressatenkreis: Wer ist betroffen?

DORA gilt für rund 20 Kategorien von Finanzunternehmen sowie für IKT-Drittdienstleister, die als kritisch eingestuft werden. Die folgende Übersicht zeigt die wichtigsten Adressatengruppen:

Adressatenkategorie	Typische Unternehmen	Regelungsrahmen
Kreditinstitute	Banken, Sparkassen, Genossenschaftsbanken	Vollständige DORA-Anwendung ab 17.01.2025
Versicherungsunternehmen	Lebens-, Sach-, Rückversicherer	Vollständige DORA-Anwendung ab 17.01.2025
Wertpapierfirmen	Broker, Investmentfirmen (MiFID II)	Vollständige DORA-Anwendung ab 17.01.2025
Zahlungsinstitute & E-Geld-Institute	Payment Service Provider, Fintechs	Vollständige DORA-Anwendung ab 17.01.2025
Zentrale Gegenparteien (CCPs)	Clearinghäuser	Vollständige DORA-Anwendung ab 17.01.2025
Krypto-Dienstleister (MiCA)	Kryptobörsen, Custody-Anbieter (soweit MiCA)	Vollständige DORA-Anwendung ab 17.01.2025
Kleine Wertpapierfirmen, Kleinstversicherer	Kleinere Institute mit vereinfachtem Profil	Vereinfachter IKT-Rahmen; Übergangsfrist bis 01.01.2027
IKT-Drittdienstleister (CTPPs)	Cloud-Anbieter, Rechenzentren, Kernsoftware	Direkte ESA-Beaufsichtigung wenn als kritisch eingestuft

Hinweis für IKT-Dienstleister

DORA schließt IKT-Drittdienstleister, die kritische Funktionen für Finanzunternehmen erbringen, erstmals in die direkte Finanzmarktaufsicht ein. Kritische IKT-Drittdienstleister (CTPPs) werden von den ESAs (EBA, EIOPA, ESMA) direkt beaufsichtigt — mit Prüfungsrechten, Empfehlungsrechten und Sanktionsmöglichkeiten. Für betroffene Cloud-Anbieter und Technologiedienstleister bedeutet das: DORA ist nicht nur ein Kundenthema — es ist ein eigenes Compliance-Thema.

© 2026 Ralf Platvoet · platvoet.org

3. Die fünf Säulen von DORA

DORA strukturiert seine Anforderungen in fünf Säulen — entsprechend den Kapiteln II bis VI der Verordnung. Sie bilden zusammen einen integrierten Rahmen für digitale operationale Resilienz, der technische, organisatorische und vertragliche Anforderungen verbindet.

Säule 1 IKT-Risikomanagement *(Art. 5–15)*

Kernanforderungen

- Formeller IKT-Risikorahmen mit Strategie, Richtlinien und Verfahren
- Vollständiges IKT-Asset-Inventar (alle Systeme, Daten, Prozesse)
- Kontinuierliche Identifikation, Schutz, Erkennung, Reaktion, Wiederherstellung
- Business Continuity Management (BCM) und IKT-Notfallpläne
- Jährliche Überprüfung und Anpassung des IKT-Risikorahmens
- Leitungsorgan trägt persönliche Verantwortung — nicht delegierbar

Praktische Umsetzung

→ IKT-Risikorahmen-Dokument formal verabschieden lassen

→ Asset-Inventar mit Kritikalitätseinstufung aufbauen

→ BCM-Plan auf IKT-Szenarien ausweiten und testen

→ Vorstand/Aufsichtsrat regelmäßig über IKT-Risiken informieren

→ Gap-Analyse gegen Art. 5–15 durchführen

Säule 2 IKT-Vorfallmanagement & Meldepflichten *(Art. 17–23)*

Kernanforderungen

- Klassifikation aller IKT-Vorfälle nach DORA-Kritikalitätskriterien
- Dreigliedrige Meldepflicht: Erstmeldung (4 h), Zwischenmeldung (72 h), Abschlussbericht (1 Monat)
- Meldung an nationale Behörde (BaFin, FMA etc.) — bei systemrelevanten Vorfällen auch an EBA
- Intern: Eskalationspfade, Kommunikationsprotokolle, Lessons Learned
- Freiwilliger Informationsaustausch zu Cyberbedrohungen (Säule 5)

Praktische Umsetzung

→ Incident-Response-Prozess auf DORA-Fristen ausrichten (4 h!)

→ Klassifikationsmatrix für Vorfälle nach DORA-RTS entwickeln

→ Meldewege zur Aufsichtsbehörde testen und dokumentieren

→ SIEM/SOC auf DORA-Reporting ausrichten

→ Tabletop-Übungen für schwere IKT-Vorfälle durchführen

Säule 3 Testen der digitalen Betriebsstabilität *(Art. 24–27)*

Kernanforderungen

- Risikobasiertes, jährliches Testprogramm für alle IKT-Systeme
- Mindestanforderungen: Schwachstellenscans, Penetrationstests, Open-Source-Analysen

Praktische Umsetzung

→ Bestehende Testpläne gegen Art. 24–25 prüfen und erweitern

→ Prüfen, ob TLPT-Pflicht besteht (BaFin/ESA-Einstufung abwarten)

© 2026 Ralf Platvoet · platvoet.org

▸ TLPT (Threat-Led Penetration Testing) für systemrelevante Institute — alle 3 Jahre ▸ TLPT nach TIBER-EU-Framework durch akkreditierte externe Tester ▸ Testergebnisse an Aufsicht melden; Mängel innerhalb definierter Fristen beheben	→ Externe TLPT-Anbieter mit TIBER-EU-Zertifizierung evaluieren → Testkalender in das IKT-Risikorahmen-Dokument integrieren → Budget für regelmäßiges Resilienztesting einplanen

Säule 4 IKT-Drittparteienrisikomanagement *(Art. 28–44)*

Kernanforderungen	Praktische Umsetzung
▸ Strategie für IKT-Drittparteienrisiko entwickeln und formal verabschieden ▸ Due-Diligence-Prüfungen vor Vertragsschluss mit IKT-Anbietern ▸ Pflichtinhalte für alle IKT-Verträge (SLAs, Prüfrechte, Exit-Strategien, Subauslagerungen) ▸ IKT-Informationsregister (alle Vertragsbeziehungen, Kritikalitätseinstufung, Subcontracting) ▸ Laufende Überwachung kritischer IKT-Drittdienstleister ▸ Exit-Strategien und Ausstiegspläne für kritische Abhängigkeiten	→ Vollständiges IKT-Informationsregister (ITS 2024/2956) aufbauen → Bestandsverträge gegen DORA-Mindestklauseln prüfen und anpassen → Konzentrations-/Klumpenrisiken bei Cloud-Anbietern analysieren → Exit-Strategien für Top-5-kritische Drittanbieter ausarbeiten → Laufende Due-Diligence-Prozesse formalisieren

Säule 5 Informationsaustausch *(Art. 45)*

Kernanforderungen	Praktische Umsetzung
▸ Freiwillige Teilnahme an Informationsaustauschvereinbarungen zu Cyberbedrohungen ▸ Austausch von Informationen über Taktiken, Techniken und Prozeduren (TTPs) von Angreifern ▸ Beteiligung an sektoralen Informationsplattformen (ISACs, nationale Strukturen) ▸ Schutz sensibler Informationen — Vertraulichkeit und Datenschutz wahren	→ Teilnahme an bestehenden ISACs prüfen (z. B. FS-ISAC für Finanzsektor) → Interne Freigabeprozesse für Informationsaustausch definieren → NDA-Strukturen und Vertraulichkeitsklauseln für Austauschformate klären → Mit BaFin/BSI abgestimmte Kommunikationskanäle etablieren

© 2026 Ralf Platvoet · platvoet.org

4. Governance: Leitungsverantwortung als DORA-Kernthema

DORA stellt eine regulatorische Besonderheit dar, die in bisherigen IT-Regelwerken so nicht verankert war: Das Leitungsorgan — also Vorstand und Aufsichtsrat — ist persönlich und unmittelbar verantwortlich für das IKT-Risikomanagement. Diese Verantwortung ist **nicht delegierbar** an die IT-Abteilung, den CISO oder externe Berater. Sie kann und soll durch diese Funktionen unterstützt werden — aber die Rechenschaftspflicht verbleibt auf Leitungsebene.

Anforderung an das Leitungsorgan	Konkreter Inhalt	Rechtsgrundlage
Formelle Verabschiedung	IKT-Risikorahmen, IKT-Strategie und wesentliche Richtlinien müssen vom Leitungsorgan förmlich beschlossen werden	Art. 5 DORA
Regelmäßige Information	Das Leitungsorgan erhält regelmäßige Berichte über IKT-Risiken, Vorfälle und Testergebnisse	Art. 5 Abs. 4 DORA
Schulungspflicht	Leitungsorganmitglieder müssen ausreichende IKT-Risikokenntnisse nachweisen und regelmäßig geschult werden	Art. 5 Abs. 4 DORA
Ressourcenverantwortung	Ausreichende Ressourcen für IKT-Sicherheit und Resilienz müssen durch das Leitungsorgan sichergestellt werden	Art. 5 Abs. 2 DORA
Persönliche Haftung	Pflichtverletzungen können zu persönlicher Haftung und aufsichtsrechtlichen Maßnahmen führen	Art. 50 ff. DORA

Praktische Implikation für Vorstände und Aufsichtsräte

DORA erfordert aktives Engagement des Leitungsorgans — nicht nur formale Zustimmung zu Berichten. Vorstandsmitglieder, die IKT-Risikothemen an den CISO delegieren und nicht selbst verfolgen, erfüllen ihre DORA-Pflichten nicht. Empfohlen werden: reguläre IKT-Risikoberichte als fester Tagesordnungspunkt, eine jährliche Schulung zu IKT-Risikothemen und eine klare Zuordnung von IKT-Resilienz-Verantwortung auf Vorstandsebene.

© 2026 Ralf Platvoet · platvoet.org

5. DORA im Regulierungskontext: Abgrenzung und Zusammenspiel

DORA existiert nicht im regulatorischen Vakuum. Es steht in engem Zusammenhang mit NIS2, dem EU Cyber Resilience Act und bestehenden nationalen Regelwerken. Die folgende Abgrenzung hilft, Doppelaufwände zu vermeiden und Synergien zu nutzen:

Regelwerk	Zielgruppe	Schwerpunkt	Verhältnis zu DORA
DORA (EU 2022/2554)	Finanzsektor (ca. 20 Kategorien) + CTPPs	Digitale operationale Resilienz, IKT-Risikomanagement	Primärrahmen für den Finanzsektor
NIS2 (EU 2022/2555)	KRITIS-Betreiber, wesentliche & wichtige Einrichtungen	Netz- und Informationssicherheit, Meldepflichten	DORA geht für Finanzsektor vor (Lex specialis)
CRA (EU 2024/2847)	Hersteller von Produkten mit digitalen Elementen	Cybersicherheit im Produktlebenszyklus	Ergänzend — betrifft IKT-Produkte, die Finanzunternehmen einsetzen
BAIT/VAIT/KAIT/ZAIT	Deutsche Finanzinstitute (BaFin-Verwaltungsvorschriften)	IKT-Risikomanagement national	Löst DORA ab als Primärrahmen; gilt ergänzend für MaRisk-Anforderungen
ISO 27001	Alle Organisationen	Informationssicherheits-Managementsystem	Komplementär; DORA-Anforderungen gehen über ISO 27001 hinaus

Entscheidend für Finanzunternehmen: DORA gilt als **Lex specialis** gegenüber NIS2 — das bedeutet, NIS2-Anforderungen sind für Finanzinstitute durch DORA vollständig abgedeckt. Eine separate NIS2-Implementierung ist für den Finanzsektor nicht erforderlich, sofern DORA vollständig umgesetzt ist. Ergänzend bleiben jedoch MaRisk-Anforderungen neben DORA anwendbar, wie die BaFin explizit klargestellt hat.

© 2026 Ralf Platvoet · platvoet.org

6. Aufsicht und Sanktionen

6.1 Nationale und europäische Aufsichtsbehörden

DORA schafft eine zweistufige Aufsichtsstruktur: Nationale Aufsichtsbehörden (NCAs) sind für Finanzunternehmen zuständig; die ESAs (EBA, EIOPA, ESMA) beaufsichtigen direkt die als kritisch eingestuften IKT-Drittdienstleister (CTPPs).

Behörde	Zuständigkeit	Befugnisse
BaFin (Deutschland)	Alle DORA-pflichtigen Finanzunternehmen in Deutschland	Prüfungsrechte, Anordnungsbefugnisse, Sanktionen, Abberufung von Leitungsorganmitgliedern
FMA (Österreich)	DORA-pflichtige Finanzunternehmen in Österreich	Gleichwertig zur BaFin; nationale Vollzugsbehörde
EBA	Kreditinstitute; Lead Overseer für CTPPs im Bankensektor	Direkte Prüfung, Empfehlungen, Zugang zu Informationen bei CTPPs
EIOPA	Versicherungsunternehmen; Lead Overseer für CTPPs im Versicherungssektor	Direkte Prüfung, Empfehlungen, Zugang zu Informationen bei CTPPs
ESMA	Wertpapierfirmen, CCPs; Lead Overseer für CTPPs im Wertpapiersektor	Direkte Prüfung, Empfehlungen, Zugang zu Informationen bei CTPPs

6.2 Sanktionsrahmen

DORA sieht einen abgestuften Sanktionsrahmen vor. Die konkreten Sanktionshöhen werden durch die nationalen Vollzugsgesetze bestimmt (in Deutschland: Finanzmarktdigitalisierungsgesetz / FinmadiG, in Kraft seit 27. Dezember 2024):

Sanktionsart	Adressat	Mögliche Maßnahmen
Verwaltungsmaßnahmen	Finanzunternehmen	Anordnungen, Verpflichtungszusagen, öffentliche Bekanntmachung (Naming & Shaming)
Bußgelder (Finanzunternehmen)	Finanzunternehmen	Bis zu 1 % des weltweiten Jahresumsatzes (täglich, bis Verstoß behoben)
Bußgelder (CTPPs)	Kritische IKT-Drittdienstleister	Bis zu 1 % des weltweiten Tagesumsatzes für max. 6 Monate
Persönliche Sanktionen	Leitungsorganmitglieder	Abberufung, Tätigkeitsverbote, persönliche Bußgelder
Prüfungspflichten	Wirtschaftsprüfer	WP müssen DORA-Compliance im Rahmen der Jahresabschlussprüfung testieren

© 2026 Ralf Platvoet · platvoet.org

Erste BaFin-Prüfungen 2025/2026

Die BaFin hat nach eigenen Angaben im ersten Jahr der DORA-Anwendung begonnen, die Umsetzung bei ausgewählten Instituten zu prüfen. Schwerpunkte der ersten Prüfungswelle sind: Vollständigkeit des IKT-Informationsregisters (Erstmeldung war bis März 2025 fällig), Governance-Strukturen und Nachweispflichten des Leitungsorgans sowie Incident-Response-Fähigkeiten. Institute, die noch keine erste Version ihres IKT-Informationsregisters eingereicht haben, sollten dies umgehend nachholen.

© 2026 Ralf Platvoet · platvoet.org

7. Implementierungspfad: Von der Gap-Analyse zur DORA-Compliance

Die folgende Roadmap beschreibt einen strukturierten Implementierungsansatz in sechs Schritten. Sie gilt sowohl für Institute, die noch in der Umsetzung sind, als auch für solche, die ihre erste Implementierungsphase abgeschlossen haben und nun in die Optimierungsphase eintreten.

Schritt 1 — Gap-Analyse (Wochen 1–4)

- Vollständige Bestandsaufnahme aller DORA-relevanten Prozesse, Systeme und Vertragsbeziehungen
- Abgleich mit den fünf Säulen und den technischen Standards (RTS/ITS)
- Priorisierung der identifizierten Lücken nach Kritikalität und Sanktionsrisiko
- Berichterstattung an das Leitungsorgan: Gap-Analyse als Vorlage für Vorstand/Aufsichtsrat

Schritt 2 — IKT-Risikorahmen aufbauen/schärfen (Monate 1–3)

- IKT-Risikorahmen-Dokument formell verabschieden (Vorstandsbeschluss)
- IKT-Asset-Inventar aufbauen: alle Systeme, Daten, Prozesse mit Kritikalitätseinstufung
- Schutzmaßnahmen nach DORA-Mindeststandards implementieren und dokumentieren
- BCM und IKT-Notfallplan auf DORA-Anforderungen ausrichten

Schritt 3 — Incident Response & Reporting ausrichten (Monate 2–4)

- Vorfallklassifikationsmatrix nach DORA-RTS 2024/1772 entwickeln
- Incident-Response-Prozess auf 4-Stunden-Erstmeldepflicht ausrichten
- Meldewege zur BaFin/NCA implementieren und testen
- SIEM/SOC-Konfiguration auf DORA-relevante Vorfallsklassen anpassen

Schritt 4 — Resilienztests etablieren (Monate 3–6)

- Risikobasiertes Testprogramm entwickeln und formell beschließen
- Schwachstellenscans und Penetrationstests in reguläre IT-Betriebsprozesse integrieren
- TLPT-Pflicht prüfen: Einstufung durch BaFin/ESA abwarten; bei Pflicht: Anbieterauswahl starten
- Testdokumentation und Behebungsnachweis als aufsichtsrechtliche Nachweisakte aufbauen

Schritt 5 — IKT-Informationsregister aufbauen (Monate 2–5)

- Vollständiges Register aller IKT-Vertragsbeziehungen gemäß ITS 2024/2956 aufbauen

© 2026 Ralf Platvoet · platvoet.org

- Kritikalitätseinstufung aller Drittanbieter nach DORA-Kriterien vornehmen
- Subauslagerungsketten dokumentieren (auch indirekte Abhängigkeiten)
- Bestandsverträge gegen DORA-Mindestklauseln (Art. 30) prüfen und anpassen
- Exit-Strategien für kritische Drittanbieter ausarbeiten

Schritt 6 — Verankern und Aufrechterhalten (dauerhaft)

- Jährliche Überprüfung und Aktualisierung des IKT-Risikorahmens
- Regelmäßige Schulungen des Leitungsorgans zu IKT-Risikothemen
- Laufendes Monitoring von RTS/ITS-Änderungen und ESA-Leitlinien
- Teilnahme an Informationsaustauschplattformen prüfen und ggf. etablieren
- DORA-Compliance als festen Bestandteil in die jährliche Abschlussprüfung integrieren

© 2026 Ralf Platvoet · platvoet.org

8. DORA-Readiness-Check: Wo steht Ihr Institut?

Der folgende Kurzcheck ermöglicht eine erste Einschätzung der DORA-Compliance-Reife. Beantworten Sie jede Frage mit Ja (✓), Teilweise (△) oder Nein (✗). Die Auswertung gibt Ihnen eine Orientierung zu Ihrem aktuellen Umsetzungsstand.

#	Frage	✓ / △ / ✗
1	Hat das Leitungsorgan den IKT-Risikorahmen formell verabschiedet?	
2	Existiert ein vollständiges IKT-Asset-Inventar mit Kritikalitätseinstufung?	
3	Wurde das IKT-Informationsregister an die zuständige NCA gemeldet?	
4	Sind Incident-Response-Prozesse auf die 4-Stunden-Erstmeldepflicht ausgerichtet?	
5	Gibt es ein risikobasiertes, dokumentiertes Testprogramm für IKT-Systeme?	
6	Wurden Bestandsverträge mit IKT-Anbietern auf DORA-Mindestklauseln geprüft?	
7	Existieren dokumentierte Exit-Strategien für kritische IKT-Drittanbieter?	
8	Wurde eine Konzentrations-/Klumpenrisikoanalyse bei Cloud-Anbietern durchgeführt?	
9	Erhält das Leitungsorgan regelmäßige Berichte über IKT-Risiken und Vorfälle?	
10	Wurden Leitungsorganmitglieder zu IKT-Risikothemen geschult?	

Auswertung

9–10 x ✓: Hohe DORA-Readiness — Fokus auf laufende Überwachung und Optimierung.

6–8 x ✓: Mittlere Readiness — Verbleibende Lücken priorisieren und schließen.

3–5 x ✓: Erhebliche Lücken — Strukturiertes DORA-Programm mit Zeitplan aufsetzen.

< 3 x ✓: Kritischer Rückstand — Sofortmaßnahmen und externe Unterstützung empfohlen.

© 2026 Ralf Platvoet · platvoet.org

9. Fazit: DORA als Chance zur Resilienz-Stärkung

DORA ist ein anspruchsvolles Regelwerk — aber kein Selbstzweck. Organisationen, die DORA konsequent umsetzen, erreichen mehr als regulatorische Compliance: Sie bauen eine robustere IKT-Infrastruktur auf, stärken ihre Widerstandsfähigkeit gegen Cyberangriffe und schaffen die Grundlagen für vertrauenswürdige digitale Finanzdienstleistungen.

Die entscheidende Verschiebung, die DORA erzwingt, ist kultureller Natur: IKT-Resilienz ist keine IT-Frage mehr — sie ist eine Führungsaufgabe. Leitungsorgane, die das internalisieren, werden DORA nicht als Bürde erleben, sondern als Rahmen für strategisch fundiertes Risikomanagement in einer zunehmend digitalen Finanzwelt.

Für IKT-Dienstleister und Technologieanbieter im Finanzumfeld gilt: DORA verändert die Spielregeln. Wer als kritischer Drittanbieter eingestuft wird, steht unter direkter europäischer Aufsicht. Wer nicht eingestuft wird, muss dennoch DORA-konforme Vertragsstrukturen, Prüfrechte und Exit-Strategien akzeptieren. DORA ist damit auch für die Technologiebranche ein strategisch relevantes Regulierungsthema.

Drei Prioritäten für DORA-Verantwortliche

1. Leitungsorgan einbinden — jetzt: DORA ist keine Delegationsaufgabe. Vorstand und Aufsichtsrat müssen aktiv und nachweislich eingebunden sein.
2. IKT-Informationsregister vervollständigen: Es ist das zentrale Nachweisdokument für Aufsichtsbehörden — und der häufigste Prüfungsschwerpunkt der ersten BaFin-Welle.
3. Drittanbieter-Verträge aktualisieren: Fehlende DORA-Klauseln sind ein bekanntes Compliance-Risiko. Priorisieren Sie kritische Vertragsbeziehungen.

© 2026 Ralf Platvoet · platvoet.org

Quellen & Weiterführende Dokumente

- Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates (DORA), 14.12.2022
- BaFin: DORA-Übersicht und Aufsichtsmitteilungen (bafin.de/dora), Stand 2025/2026
- BaFin: Aufsichtsmitteilung zur Umsetzung von DORA — IKT-Risikomanagement und Drittparteienrisiko (21.08.2025)
- Finanzmarktdigitalisierungsgesetz (FinmadiG), in Kraft seit 27.12.2024
- EBA/EIOPA/ESMA: Regulatory Technical Standards (RTS) und Implementing Technical Standards (ITS) zu DORA, 2024
- ITS 2024/2956: Informationsregister für IKT-Drittdienstleister
- EIOPA: DORA-Übersicht (eiopa.europa.eu/dora)
- Gleiss Lutz: DORA — IKT Risk Compliance Obligations for the Financial Sector, 2025
- CGI: DORA — Harmonisierung der finanziellen Stabilität in Europa, September 2025

Über den Autor

Ralf Platvoet ist Diplom-Ökonom und Inhaber von PPI – Platvoet Performance Intelligence. Er berät Organisationen zu Cyber-Compliance (DORA, NIS2, EU Cyber Resilience Act, ISO 27001), Strategic Portfolio Management und PMO-Advisory. Sein Beratungsschwerpunkt liegt auf der Verbindung regulatorischer Anforderungen mit strategischer Steuerungsfähigkeit — für Finanzunternehmen ebenso wie für IKT-Dienstleister im regulierten Umfeld.

Weitere Whitepapers, Tools und Ressourcen: **platvoet.org**

Haftungsausschluss

Dieses Whitepaper dient ausschließlich allgemeinen Informationszwecken und stellt keine Rechts- oder Compliance-Beratung dar. Die regulatorischen Anforderungen aus DORA und den zugehörigen technischen Standards sind komplex und institutsspezifisch. Für die Beurteilung der eigenen Compliance-Situation empfehlen wir die Einbindung qualifizierter Rechts- und Compliance-Berater sowie die direkte Konsultation der zuständigen Aufsichtsbehörden.

© 2026 Ralf Platvoet · platvoet.org