

DORA Jahresabschlußprüfung - Was sind die Prüfungsfelder?

Christoph Gruber

2026-01-16

Agenda

1. Rechtsrahmen und Prüfungspflicht
2. Die fünf Säulen der DORA-Prüfung
3. Kategorien und Proportionalität
4. Typische Mängel aus den ersten Prüfungen
5. Erleichterungen für die Erstprüfung GJ 2025 (Deutschland)
6. Praktische Empfehlungen

Teil 1: Rechtsrahmen und Prüfungspflicht

DORA - Der neue Standard

Digital Operational Resilience Act Verordnung (EU) 2022/2554

- In Kraft seit 16.01.2023
- **Anwendbar seit 17.01.2025**
- Gilt unmittelbar in allen EU-Mitgliedstaaten
- Ersetzt nationale IT-Rahmenwerke (xAIT)

Nationale Umsetzung

	Deutschland	Österreich
Gesetz	FinmadiG	DORA-VG
Aufsicht	BaFin + Bundesbank	FMA + OeNB
xAIT- Status	BAIT bis 31.12.2026; KAIT, VAIT, ZAIT aufgehoben 16.01.2025	Nie eingeführt

Prüfungspflicht im Jahresabschluss

Die DORA-Prüfung ist **keine separate Prüfung**, sondern Teil der Jahresabschlussprüfung.

Erstmalige Anwendung: - Geschäftsjahre, die nach dem 31.12.2024 beginnen - Bei kalendergleichem GJ: Prüfung für GJ 2025

Prüfungsgegenstand (DE)

Gemäß FinmadiG prüft der Abschlussprüfer die Einhaltung von:

**Artikel 5-14, 16-19, 23-25, 28-30, 45 Abs. 3 DO-
RA**

sowie zugehörige Delegierte Verordnungen

Prüfungsstandard

Deutschland: - IDW EPS 528 (08.2025) - Konsultation abgeschlossen (31.10.2025) - Finalisierung als IDW PS 528 erwartet - Prinzipienorientierter Ansatz - Basiert auf IDW PS 526

Österreich: - Kein separater Prüfungsstandard - Direkte DORA-Anwendung

Teil 2: Die fünf Säulen der DORA-Prüfung

Überblick: Fünf Säulen

1. **IKT-Risikomanagement** (Art. 5-16)
2. **IKT-Vorfallsmanagement** (Art. 17-23)
3. **Testen der digitalen Resilienz** (Art. 24-27)
4. **IKT-Drittparteienrisiko** (Art. 28-30)
5. **Informationsaustausch** (Art. 45)

Säule 1: IKT-Risikomanagement

Kernprüfungsfelder:

- Governance und Letztverantwortung Leitungsorgan (Art. 5)
- IKT-Risikomanagementrahmen (Art. 6)
- DOR-Strategie (Art. 6 Abs. 8)
- Asset-Inventar und Kritikalitätsbewertung (Art. 8)
- Sicherheitsrichtlinien (Art. 9)
- Business Continuity und Recovery (Art. 11-12)

Säule 1: Typische Nachweise

Prüfungsfeld	Nachweise
Governance	Geschäftsordnung, Kompetenzmatrix
IKT-RM-Rahmen	Policy-Dokument, Review-Protokolle
DOR-Strategie	Strategie-Dokument mit 8 Pflichtelementen
Asset-Inventar	CMDB, Asset-Register
BCP/DRP	Pläne, BIA, Testprotokolle

Säule 2: IKT-Vorfallsmanagement

Kernprüfungsfelder:

- Incident-Management-Prozess (Art. 17)
- Klassifizierungsmethodik (Art. 18)
- Meldeverfahren und -fristen (Art. 19)
- Vorfallsregister (Art. 17 Abs. 3)

Säule 2: Meldefristen

Meldung

Frist

Erstmeldung

4h nach Klassifizierung
/ 24h nach Kenntnis

Zwischenmeldung

72 Stunden

Abschlussmeldung

1 Monat

Template: DVO (EU) 2025/302

Säule 3: Testen der digitalen Resilienz

Kernprüfungsfelder:

- Testprogramm als Teil des IKT-RM (Art. 24)
- Jährliche Tests kritischer Systeme (Art. 25)
- Testarten: Vulnerability Scans, Pentests, Szenario-Tests
- TLPT alle 3 Jahre (Art. 26-27) - nur Kategorie D

Säule 3: Testarten nach Art. 25

- Schwachstellenbewertungen und -scans
- Open-Source-Analysen (SBOM)
- Netzwerksicherheitsbewertungen
- Gap-Analysen
- Physische Sicherheitsüberprüfungen
- Penetrationstests
- Szenariobasierte Tests
- End-to-End-Tests

Säule 4: IKT-Drittparteienrisiko

Kernprüfungsfelder:

- Third-Party-Risk-Strategie (Art. 28 Abs. 2)
- **Informationsregister** (Art. 28 Abs. 3)
- Due Diligence (Art. 28 Abs. 4)
- Vertragliche Mindestinhalte (Art. 30)
- Exit-Strategien (Art. 28 Abs. 8)
- Konzentrationsrisiko (Art. 29)

Säule 4: Informationsregister

Pflichtbestandteile (DVO 2024/2956):

- Alle IKT-Drittanbieterverträge
- Kritikalitätsbewertung je Vertrag
- Unterstützte Funktionen
- Standorte der Datenverarbeitung
- Exit-Optionen

Erstmeldung: 31.03.2025

Säule 5: Informationsaustausch

Prüfungsfeld (Art. 45 Abs. 3):

- Freiwillige Teilnahme an Austauschvereinbarungen
- Vertraulichkeitsregelungen (NDAs)
- Meldung der Teilnahme an Aufsicht

Niedrigere Prüfungsrelevanz als Säulen 1-4

Teil 3: Kategorien und Proportionalität

Proportionalitätsgrundsatz (Art. 4)

Die Anforderungen sind abgestuft nach: - Größe und Gesamtrisikoprofil - Art, Umfang und Komplexität der Dienstleistungen - Kritikalität für das Finanzsystem

Vier Kategorien

Kategorie	Beschreibung
D	Systemrelevant (G-SII, O-SII, SSM, >30 Mrd.)
A	Reguläre Finanzunternehmen
B	Kleine, nicht verflochtene Institute
C	Kleinstunternehmen (<10 MA, ≤2 Mio. EUR)

Anforderungsmatrix

Anforderung	D	A	B	C
Vollständiger IKT-RM-Rahmen	✓	✓	○	—
DOR-Strategie	✓	✓	—	—
Drei-Linien-Modell	✓	✓	—	—
Jährliche Überprüfung	✓	✓	○	○
TLPT (alle 3 Jahre)	✓	—	—	—
Vollständiges Register	✓	✓	✓	○

✓ = Pflicht | ○ = Vereinfacht | — = Befreit

Kategorie C - Vereinfachungen

Kleinstunternehmen nach Art. 16: - Kein
Drei-Linien-Modell erforderlich - Keine separate
IKT-Risikokontrollfunktion - Keine DOR-Strategie -
Periodische statt jährliche Überprüfung - Vereinfachtes
Asset-Register - Basis-Notfallplan ausreichend
Aber: Meldepflichten für Vorfälle bleiben unverändert!

Teil 4: Typische Mängel aus den ersten Prüfungen

Häufige Feststellungen GJ 2025

1. **Governance:** Letztverantwortung des Leitungsorgans nicht klar dokumentiert
2. **Kritische Funktionen:** Unvollständige Identifikation und Bewertung
3. **Informationsregister:** Unvollständig, fehlende Kritikalitätsbewertung
4. **Exit-Strategien:** Nicht oder nur rudimentär vorhanden
5. **Vertragsklauseln:** Art. 30-Mindestinhalte fehlen in Altverträgen

Mängel im Detail: Governance

Typische Feststellung: - Verantwortung für IKT-Risiken nicht explizit in Geschäftsordnung - Keine dokumentierten IKT-Schulungen des Vorstands - Budget für IKT nicht separat ausgewiesen

Empfehlung: - Geschäftsordnung ergänzen - Schulungsnachweise dokumentieren - IKT-Budgetplanung formalisieren

Mängel im Detail: Kritische Funktionen

Typische Feststellung: - Keine vollständige Liste kritischer/wichtiger Funktionen - Kritikalitätskriterien nicht definiert - Mapping zu IKT-Assets fehlt

Empfehlung: - Funktionskatalog erstellen - Kritikalitätskriterien dokumentieren - Abhängigkeitsmatrix pflegen

Mängel im Detail: Informationsregister

Typische Feststellung: - Nicht alle IKT-Verträge erfasst -
Kritikalitätsbewertung fehlt - Standorte der
Datenverarbeitung unbekannt

Empfehlung: - Vollständige Vertragserfassung -
Kritikalitätsbewertung je Vertrag - Aktive Abfrage bei
Dienstleistern

Teil 5: Erleichterungen Erstprüfung GJ 2025

Erleichterungen Deutschland (BaFin/IDW)

- 1. Abgestellte Mängel:** - Mängel, die bis Jahresende vollständig behoben wurden - Keine Berichtspflicht erforderlich - Aber: Dokumentation in Arbeitspapieren
- 2. Verkürzte Wirksamkeitsprüfung:** - Bei unterjähriger DORA-Implementierung zulässig - Angemessene Prüfungstiefe nach Ermessen

Erleichterungen Deutschland (Fortsetzung)

3. Abweichendes Geschäftsjahr: - Zeitraum 17.01.2025 bis GJ-Ende - BAIT-Anforderungen können geprüft werden - KAIT, VAIT, ZAIT bereits aufgehoben

4. Proportionalität: - Explizit in PrüfV verankert - Prüfungsumfang nach Risikoprofil

Situation Österreich

- **Keine expliziten Erleichterungen** kommuniziert
- Sofortige Vollintegration erwartet
- Im Zweifel: Abstimmung mit FMA empfohlen
- Kooperativer Aufsichtsansatz ("Reden wir über Aufsicht")

Teil 6: Praktische Empfehlungen

Empfehlung 1: “Always Audit Ready”

Dokumentation kontinuierlich pflegen - nicht erst vor der Prüfung:

- Asset-Register aktuell halten
- Vertragsregister laufend pflegen
- Vorfälle zeitnah dokumentieren
- Testberichte archivieren

Empfehlung 2: Frühzeitige Abstimmung

- Erwartungen des Prüfers klären
- Prüfungsschwerpunkte abstimmen
- Dokumentationsformate vereinbaren
- Zeitplan koordinieren

Empfehlung 3: Prioritäten für kleinere Institute

1. **Robustes Register** - Alle IKT-Verträge erfassen
2. **Präzise Kritikalitäten** - Funktionen und Assets bewerten
3. **Klare Meldewege** - Vorfallsmeldung sicherstellen
4. **Vertragsanpassungen** - Art. 30-Klauseln nachverhandeln
5. **Exit-Prozeduren** - Zumindest für kritische Dienstleister

Empfehlung 4: Dokumentation

Bereich	Minstdokumentation
Governance	Geschäftsordnung, Kompetenzmatrix
IKT-RM	Policy, Review-Protokolle
Assets	Register mit Kritikalität
Vorfälle	Vorfallsregister, Meldungen
Drittparteien	Informationsregister, Exit-Pläne

Sanktionen bei Verstößen

- Bis zu **1% des weltweiten Jahresumsatzes**
- Naming & Shaming (Veröffentlichung)
- Persönliche Haftung des Leitungsorgans möglich

Zusammenfassung

1. DORA-Prüfung ist Teil der Jahresabschlussprüfung
2. Fünf Säulen mit abgestuften Anforderungen
3. Proportionalität nach vier Kategorien
4. Erstprüfungserleichterungen in DE nutzen
5. Kontinuierliche Dokumentation statt Ad-hoc-Aktionen

Vielen Dank für Ihre Aufmerksamkeit!

Fragen?

Christoph Gruber

ISM - Information Security Management Consulting

christoph.gruber@ismc.at

+43 664 2111061

Stand: Jänner 2026

Anhang: Wichtige Rechtsquellen

- Verordnung (EU) 2022/2554 (DORA)
- DVO (EU) 2024/1772 (Klassifizierung)
- DVO (EU) 2024/1774 (IKT-RM)
- DVO (EU) 2024/2956 (Informationsregister)
- DVO (EU) 2025/302 (Meldevorlagen)
- FinmadiG (Deutschland)
- DORA-VG (Österreich)
- IDW EPS 528 (08.2025)