GUIDE 2025/2026

DORA guide for the financial sector

The Digital Operational Resilience Act, explained plainly

notivia GmbH

Edition 2025/2026

Contents

1 What is DORA? 3

1.1 The regulation in plain words 3

1.2 The five pillars of DORA 3

1.3 DORA vs. BAIT/KAIT — what is new? 4

1.4 How it sits alongside other rules 4

2 Are you in scope? 6

3 The road to compliance — seven phases 8

4 What does DORA cost? 10

5 The ten most common mistakes 12

6 Readiness check: are you ready? 14

7 Glossary 16

8 Your next step 18

1 What is DORA?

1.1 The regulation in plain words

DORA stands for the **Digital Operational Resilience Act** — the EU regulation on digital operational resilience for the financial sector (Regulation (EU) 2022/2554). Since **17 January 2025** it has been binding, and it applies directly in every EU member state — with no national transposition.

The aim: the European financial sector should be able to withstand cyber attacks and IT outages. DORA requires financial entities and their ICT third-party providers to reach a **demonstrable level of IT resilience** — and to make it auditable by the supervisory authorities (in Germany: BaFin and the Bundesbank).

> **The core idea:** DORA does not ask "how expensive is your IT?" but "what happens when it fails — and how quickly are you able to operate again?"

The sanctions are severe: periodic penalty payments of up to **1 % of average daily worldwide turnover**. Senior managers are personally liable. Reporting major ICT incidents is mandatory — late or missing reports are sanctionable in their own right.

1.2 The five pillars of DORA

DORA groups its requirements into five central areas:

1. **ICT risk management** (Art. 5–16) — a framework for identifying, protecting against, detecting, responding to and recovering from ICT risks.
2. **Reporting ICT-related incidents** (Art. 17–23) — harmonised reporting processes and deadlines for major incidents towards the competent authorities.
3. **Digital Operational Resilience Testing** (Art. 24–27) — regular testing, including threat-led penetration testing (TLPT) for systemically important institutions.
4. **Managing ICT third-party risk** (Art. 28–44) — the register of information, contractual requirements and the oversight framework for critical third-party providers.
5. **Information sharing** (Art. 45) — voluntary sharing of cyber threat information between financial entities.

> **An easy way to remember it:** the five pillars map the whole cycle: *know your risks* (1), *report incidents* (2), *test your resilience* (3), *control your supply chain* (4), *learn together* (5).

1.3 DORA vs. BAIT/KAIT — what is new?

In Germany, BAIT (the supervisory requirements for IT in banks) and KAIT (for asset management companies) have governed IT risk management for years. DORA **replaces** those national rules with one EU-wide standard.

22,000+
financial entities in scope across the EU

5
pillars (Art. 5–45)

1 %
maximum annual penalty, of worldwide turnover

The most important changes compared with BAIT and KAIT:

- **EU harmonisation** — one set of standards instead of a national patchwork.
- **A wider scope** — for the first time this also covers crypto-asset service providers, crowdfunding service providers, central securities depositories and credit rating agencies.
- **TLPT is mandatory** for systemically important financial institutions, at least every three years.
- **Register of information (RoI)** — complete documentation of every ICT provider, filed annually with BaFin.
- **Oversight Framework** for critical ICT third-party providers — direct European supervision for the first time.

1.4 How it sits alongside other rules

Rules	Focus	Scope
DORA	ICT resilience, financial sector	EU-wide, binding
NIS-2	Cybersecurity, critical sectors	EU, but not finance — DORA applies there
ISO 27001	Information security in general	Voluntary (certification)
BAIT/KAIT	IT supervision in Germany (national)	Replaced by DORA
MaRisk	Overall banking supervision in Germany	Remains in place, as a complement

Worth knowing: An existing ISO 27001 ISMS covers around 60 % of the DORA requirements. ICT risk management (pillar 1) in particular overlaps heavily. If you hold ISO 27001 you save 40 to 50 % of the implementation effort for DORA.

2 Are you in scope?

DORA applies to 21 categories of financial entity (Art. 2). If you fall into one of them you are covered, whatever your size. ICT third-party providers are covered as well, as soon as they supply services to those entities.

A. Financial entities covered directly

The core financial sector

- Credit institutions (banks, savings banks, private banks)
- Payment service providers, acquirers and e-money institutions
- Investment firms
- Insurance and reinsurance undertakings
- Pension funds and institutions for occupational retirement provision

Capital market infrastructure

- Central securities depositories (CSDs)
- Central counterparties (CCPs)
- Trading venues
- Trade repositories

New categories, regulated for the first time

- Crypto-asset service providers under MiCA
- Crowdfunding service providers
- Custodians of crypto-assets
- Data reporting service providers
- Credit rating agencies

B. ICT third-party providers covered indirectly

Every IT company supplying services to financial institutions falls under DORA indirectly, through the contractual requirements in Art. 30. That includes:

- Cloud service providers (IaaS, PaaS, SaaS)
- Data centres and colocation providers
- Managed security service providers (MSSPs)
- Software vendors with critical financial applications
- Outsourcing providers, core banking systems for example

> **A special case:** Entities designated by the ESAs as **critical ICT third-party providers** come under direct European supervision — with correspondingly high requirements for governance, resilience and transparency.

C. Exemptions (proportionality)

Microenterprises and smaller investment firms may apply simplified requirements (Art. 16). They are not exempt altogether — only relieved on documentation and the extent of testing.

> *A real example: a payment service provider with 45 staff and €18 million turnover has to implement DORA in full — the ICT risk management framework, incident reporting and the register of information included. Its size reduces only the extent of testing, not the basic duties.*

What does being in scope actually mean?

Every entity in scope has had **immediately binding duties** since 17 January 2025:

- A complete ICT risk management framework (governance, policy, register)
- An incident response plan with rehearsed reporting routes (initial, intermediate and final notification)
- Filing the register of information with the competent authority every year
- Reviewing every ICT service contract for DORA conformity
- Regular resilience testing — TLPT for systemically important entities

3 The road to compliance — seven phases

Implementing DORA is a company-wide programme, not an IT project. Depending on where you start, full implementation takes **four to twelve months**.

1. **Gap analysis and scoping**

   Take stock against all five pillars. Prioritise the gaps by risk and effort. If ISO 27001 is in place, 60 % of the groundwork already exists. Three to six weeks.

2. **Build ICT governance**

   Settle the management body's responsibilities, appoint a DORA officer, adopt the policies. Management carries demonstrable ultimate responsibility (Art. 5), and its training is mandatory. Four to six weeks.

3. **Implement ICT risk management**

   Identify, assess and treat risks. Build the asset register. Put protective measures in place, technically and organisationally. Update the business continuity and disaster recovery plans. Three to five months.

4. **Build the register of information**

   A complete register of every ICT third-party provider with its criticality, contract conformity and substitution plans, in the harmonised ESA format, filed with BaFin every year. Two to three months, alongside phase 3.

5. **Manage the ICT provider contracts**

   Review and amend every existing ICT contract (Art. 30: security clauses, audit rights, exit strategies, rules on subcontracting). Sign new contracts only in DORA-compliant form. Two to four months.

6. **Incident response and reporting**

   Classify major incidents against the ESA taxonomy. Set up the process for initial, intermediate and final notifications and the reporting route to the BaFin and ESMA portals. Run tabletop exercises. One to two months.

7. **Establish resilience testing**

   Basic testing: regular vulnerability scans and penetration tests. Advanced: threat-led penetration testing every three years for systemically important institutions. Document and follow up. Ongoing.

> **Tip:** Start the gap analysis and the register of information at the same time. The register is the single most time-consuming piece of work — the earlier you begin, the calmer the final stretch. Many firms underestimate it by half.

4 What does DORA cost?

DORA compliance costs more than other compliance regimes, because the regulatory pressure is greater. The table below shows realistic ranges:

Type of institution	Total cost*	Timeframe	Internal effort
Small (<50 staff)	**€14,900–19,000**	4–6 months	8–12 hrs/week
Mid-sized (50–249)	**€19,000–27,000**	5–8 months	12–18 hrs/week
Medium (250–999)	**€27,000–40,000**	7–10 months	16–26 hrs/week
Large (1,000–4,999)	**€40,000–62,000**	9–14 months	½–1 FTE
Systemically important (5,000+)	**from €62,000**	12–18 months	1+ FTE

* Includes consulting, building the framework, producing the register, amending contracts and setting up incident management. Excludes the TLPT cycle (from €18,000 per cycle, separately).

What drives the cost?

- **The number of ICT providers:** the more providers, the more work the register and the contract review.
- **An existing ISMS (ISO 27001, BAIT or KAIT):** cuts implementation cost by 30 to 50 %.
- **How critical the institution is:** systemically important firms have to carry out TLPT (€18,000–60,000 per cycle).
- **How much is outsourced:** an extensive cloud or managed-services setup raises the complexity.

Running costs after implementation

Allow **25 to 35 % of the implementation cost per year** to keep it running. On top of that:

- Updating and filing the register of information each year
- TLPT (systemically important entities): every three years
- Incident handling: 30 to 100 person-hours per incident
- An external ICT risk officer (optional): from €499 a month

In the interest of transparency: Others often quote €80,000–250,000 for a DORA project. Our approach, with an ISMS platform and AI-supported documentation, delivers a clear cost advantage at the same quality — as our references in the financial sector show.

5 The ten most common mistakes

From guiding a good many DORA projects, we know the usual stumbling blocks:

1. **Starting too late**
   “We are not systemically important yet, we can wait.” The supervisor is already looking — missing basic compliance draws findings straight away.

2. **Underestimating the register of information**
   The register looks simple but is highly detailed: contract, service, location and substitution data for every third-party provider. Typically 40 to 80 person-days.

3. **BAIT-compliant means DORA-compliant?**
   No. DORA is stricter on third-party management, incident reporting and testing. An existing BAIT implementation is a good basis but not full coverage.

4. **Leaving old contracts untouched**
   Art. 30 requires specific clauses. Older cloud and managed-services contracts often do not contain them. Renegotiation drags on for three to six months per supplier.

5. **Never rehearsing the reporting process**
   The deadlines — 24 hours initial, 72 hours intermediate, one month final — are tight. Without a tabletop exercise, the first incident goes wrong.

6. **Treating DORA as an IT project**
   DORA touches compliance, legal, procurement, risk, internal audit and the board. An IT team on its own will founder on governance and third-party management.

7. **Classifying incidents wrongly**
   The ESA taxonomy for major incidents is intricate. Getting it wrong leads to mistaken reports or to none at all — both are sanctionable.

8. **Management responsibility on paper only**
   The management body has to steer ICT risk management actively and be trained demonstrably. “Signed off by the board” is not enough.

9 **Putting TLPT off**

Systemically important institutions have to evidence TLPT every three years. Qualified providers are scarce, so planning ahead is essential.

10 **Treating documentation as optional**

Supervisory reviews run on documents. Missing evidence produces findings immediately — whatever your actual security posture.

6 Readiness check: are you ready?

Answer the following ten questions honestly, yes or no. The result shows your DORA maturity.

1. **Do you have a documented ICT risk management framework?**
   The basis under Art. 5–6 — policy, processes, responsibilities.

2. **Is a complete register of information in place?**
   Every ICT provider, service and contract, in the harmonised ESA format.

3. **Do all your ICT contracts meet the Art. 30 requirements?**
   Security, audit rights, exit and subcontracting clauses — documented and reviewed.

4. **Is there an incident response plan with rehearsed reporting routes?**
   24-hour initial, 72-hour intermediate, one-month final report — with clear ownership.

5. **Do you classify incidents against the ESA taxonomy?**
   “Major” versus “significant”, against harmonised thresholds.

6. **Do you carry out resilience testing regularly?**
   Basic tests yearly, TLPT every three years for systemically important entities.

7. **Has your management body received documented DORA training?**
   Art. 5(2) — the management body has to be able to evidence it.

8. **Have you appointed a DORA or ICT risk officer?**
   Responsible in practice for the framework and for reporting.

9. **Are there documented business continuity and disaster recovery plans?**
   Tested, kept current, with clear RTO and RPO targets.

10. **Are critical third-party providers identified and actively managed?**
    Including regular audits and substitution plans.

Your yes answers	Assessment	Recommendation
0–3 × yes	**Acutely exposed**	You need to start building in a structured way now. Priority: gap analysis and the register. Expect eight to fourteen months.
4–6 × yes	**Partly prepared**	Focus on the gaps — usually third parties and incident reporting. Five to eight months.
7–10 × yes	**A good basis**	Refinement and preparing for review. Three to five months to full conformity.

DORA compliance is achievable — but only with structured planning. If you have questions, or your position is unclear, a free first conversation will help.

7 Glossary

The key DORA terms, explained plainly:

DORA

Digital Operational Resilience Act — Regulation (EU) 2022/2554 on operational resilience in the financial sector.

ICT

Information and communication technology — hardware, software, networks, cloud and data processing.

Register of information (RoI)

The central register of all ICT third-party providers, in harmonised form. Filed with BaFin every year.

TLPT

Threat-led penetration testing — a realistic penetration test based on the current threat picture. Mandatory for systemically important institutions.

Critical ICT third-party provider

A provider designated as critical by the European Supervisory Authorities. Subject to direct European supervision.

Oversight Framework

The European supervisory regime for critical ICT third-party providers (Art. 31–44).

Major incident

An ICT incident whose effects exceed the thresholds — clients affected, data lost, reputation damaged. It has to be reported.

BaFin

The German Federal Financial Supervisory Authority — responsible for DORA supervision in Germany.

ESA

European Supervisory Authorities — EBA, ESMA and EIOPA — which issue the implementing acts for DORA.

BAIT/KAIT

The German supervisory requirements for IT in banks and in asset management companies — the predecessor rules, replaced by DORA.

RTO / RPO

Recovery time objective and recovery point objective — the recovery targets.

Proportionality

The DORA requirements scale with size and complexity. Microenterprises may use simplified models.

MiCA

Markets in Crypto-Assets Regulation — the EU rules on crypto-assets. Relevant to DORA for crypto service providers.

Substitution plan

A documented plan for replacing a critical provider in a crisis.

8 Your next step

You have read this guide — that is the first step already. Implementing DORA in a structured way reduces regulatory risk, avoids fines and protects your management from personal liability.

A free first conversation

In 30 minutes, with no obligation, we work out together:

✓ Where do you stand against the five DORA pillars?

✓ Which gaps come first?

✓ What timeframe and budget are realistic?

✓ What does DORA mean for your third-party relationships?

No sales pitch, no pressure — just an honest assessment.

The quick DORA check

At **iso-easy.de** you can check in three minutes whether DORA applies to you and get a first view of the cost — without giving any contact details.

Contact

Web: iso-easy.de

Phone: +49 711 35 15 705

E-mail: feedback@iso-easy.de

iso-easy.de

iso-easy is part of notivia GmbH.

With more than 30 years of experience in IT consulting and information security we support financial entities in implementing DORA, NIS-2, ISO 27001 and neighbouring standards — pragmatically, transparently and as equals.

© 2025/2026 notivia GmbH — **iso-easy.de** | All rights reserved.