COMPLIANCE CHECKLIST

DORA compliance checklist

Digital Operational Resilience Act (Regulation 2022/2554)

Jurisdiction: EU financial entities + their ICT third-party service providers

Programme details

ORGANISATION NAME

[Organisation name]

ASSIGNED TO

[Assigned to]

TARGET COMPLETION DATE

[Target completion date]

REVIEWED BY

[Reviewed by]

REVIEW DATE

[Date]

Who DORA applies to

EU financial entities including credit institutions, payment institutions, e-money institutions, investment firms, insurers, reinsurers, AIFs, UCITS, crypto-asset service providers under MiCA, and central counterparties. Also applies to critical ICT third-party service providers under EU oversight.

DORA checklist

STEP 1
- [ ] Define the in-scope DORA perimeter (entity categories + critical third parties).

STEP 2
- [ ] Establish the ICT risk management framework and assign management body responsibility.

STEP 3
- [ ] Maintain a register of ICT systems, processes, and the people responsible.

STEP 4
- [ ] Build the ICT-related incident classification, management, and reporting workflow.

STEP 5
- [ ] Define and document the digital operational resilience testing programme.

STEP 6
- [ ] For significant entities: conduct threat-led penetration testing (TLPT) every 3 years.

STEP 7
- [ ] Maintain the ICT third-party register and contractual arrangements per Article 28.

STEP 8
- [ ] Manage concentration risk and exit strategies for critical third-party dependencies.

STEP 9

- [ ] Submit annual reports to the competent authority covering all five pillars.

STEP 10

- [ ] Update the framework based on incident learnings, regulatory technical standards, and supervisory expectations.

FAQ

What is the DORA regulation?

The DORA regulation is the Digital Operational Resilience Act - EU Regulation 2022/2554. It is the binding EU law that establishes a unified ICT operational-resilience framework for financial entities and critical ICT third-party service providers. DORA entered into force on 16 January 2023 and became applicable on 17 January 2025. The five pillars are ICT risk management, ICT-related incident reporting, digital operational resilience testing, ICT third-party risk management, and information sharing on cyber threats.

When did DORA take effect?

DORA entered into force on 16 January 2023 and became applicable on 17 January 2025. From that date, in-scope financial entities and critical ICT third-party providers must comply with the full regulation and the associated regulatory technical standards (RTS) and implementing technical standards (ITS).

Who counts as a "critical ICT third-party service provider"?

The European Supervisory Authorities (ESAs) designate critical ICT TPPs (CTPPs) under Article 31 - hyperscale cloud providers, major SaaS vendors, and core banking software providers being the obvious candidates. CTPPs face direct EU oversight regardless of whether their financial-entity customers each subject them to oversight.

What is Threat-Led Penetration Testing (TLPT)?

TLPT is realistic, intelligence-driven testing of an entity's ICT systems and processes by skilled "ethical hackers" using TTPs (tactics, techniques, procedures) of real threat actors. DORA requires TLPT every 3 years for significant entities under Article 26, aligned with the TIBER-EU framework where relevant.

How does DORA interact with the NIS2 Directive?

DORA is the lex specialis for the financial sector - where DORA applies, it overrides NIS2 obligations for the same matters. Financial entities should map their obligations under both and document the DORA / NIS2 boundary in their compliance programme.

Source: https://ba-copilot.com/compliance/dora-compliance-checklist. Tick each item as it is completed and add the named owner.