DORA vendor management checklist

The seven obligations in Articles 28 to 30 of the Digital Operational Resilience Act (Regulation (EU) 2022/2554), as things a financial entity must be able to show. DORA has applied since 17 January 2025. Taken from www.riskxchange.co/dora-third-party-risk-management, last reviewed 14 November 2026 by Darren Craig.

This checklist is a working aid, not legal advice. Check each obligation against the regulation and your competent authority's guidance.

1. Manage ICT third-party risk inside your ICT risk framework (Article 28(1) and (2))

- [ ] A strategy on ICT third-party risk, reviewed regularly
- [ ] A documented policy for arrangements that support critical or important functions
- [ ] The management body's responsibility for ICT risk recorded, whatever is contracted out

2. Maintain a register of information on all ICT arrangements (Article 28(3))

- [ ] Every contractual arrangement for ICT services on the register, not only critical ones
- [ ] Maintained at entity, sub-consolidated and consolidated level
- [ ] Ready to provide to the competent authority on request, in the current reporting format

3. Report annually, and notify planned critical arrangements (Article 28(3))

- [ ] At least yearly: new arrangements, categories of provider, types of arrangement, services and functions covered
- [ ] The authority informed in good time of any planned arrangement supporting a critical or important function
- [ ] The authority informed when an existing function becomes critical or important

4. Run due diligence before you sign (Article 28(4) and (5))

- [ ] Provider suitability assessed before the arrangement is entered into
- [ ] Contracts only with providers that apply appropriate information security standards
- [ ] For critical or important functions, the provider's standards given due consideration

5. Carry the specified contractual provisions (Article 30)

- [ ] The provisions required in every ICT contract
- [ ] The additional provisions where the arrangement supports a critical or important function

6. Assess concentration risk before contracting (Article 29)

- [ ] A preliminary assessment of ICT concentration risk
- [ ] Providers that are not easily substitutable, and multiple arrangements with the same or connected providers, covered
- [ ] Subcontracting chains assessed, including subcontractors outside the EU

7. Hold exit strategies for critical or important functions (Article 28(8))

- [ ] Documented exit strategies covering provider failure, deterioration in quality, business disruption and the termination grounds in Article 28(7)
- [ ] A transition that does not disrupt the business or breach regulatory requirements
- [ ] Exit plans tested and reviewed periodically

RiskXchange builds the register, the due diligence record and the board report from live supplier data. See www.riskxchange.co/dora-third-party-risk-management and www.riskxchange.co/pricing/platform.