DORA THIRD-PARTY RISK MANAGEMENT CHECKLIST

Compliance for financial entities under Chapter V

TPSaaS

www.tpsaas.io

Who This Applies To (Article 2(a)–(w) financial entities)

DORA applies to a wide range of financial entities. Here's a list of the specified types:

- Credit institutions
- Payment institutions
- Account information service providers
- Electronic money institutions
- Investment firms
- Crypto-asset service providers
- Central securities depositories (CSDs)
- Central counterparties (CCPs)
- Trading venues
- Trade repositories
- Alternative investment fund managers (AIFMs)
- Management companies of UCITS
- Insurance and reinsurance undertakings
- Insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries
- Institutions for occupational retirement provision (IORPs)
- Credit rating agencies
- Administrators of critical benchmarks
- Crowdfunding service providers
- Securitisation repositories
- ICT third-party service providers

Mandatory Actions – Exact Requirements (no fluff)

Here are the mandatory actions required for DORA compliance, as detailed in Chapter V (Articles 28-30):

1. **Adopt ICT Third-Party Risk Strategy & Policy (Art. 28(2-3))**
    - Map & manage ICT third-party risk as part of overall risk management.
    - Adopt & regularly review a comprehensive strategy.
    - Documented strategy for ICT third-party risk.
    - Proportionate to size, complexity & overall risk profile.
2. **Pre-contractual Due Diligence & Risk Assessment (Art. 28(4), 29)**
    - Assess concentration risk (Art. 28(5)).
    - Assess all relevant risks before contractual agreements.
    - Documented risk assessments reviewed regularly.
3. **Mandatory Contractual Clauses – ALL contracts (Art. 30(2))**
    - Full description of functions.
    - Locations where functions are performed (including potential data).
    - Service levels.
    - Rights of access, inspection & audit.
    - Reporting obligations of ICT third-party service providers.
    - Cooperation duties.
    - Termination rights and exit strategies.
    - Ensuring access, recovery, and return of data in case of insolvency, resolution or discontinuation of business of the ICT third-party service provider.
4. **EXTRA Clauses – Critical or Important Functions only (Art. 30(3))**
    - Service provider's participation in threat intelligence sharing arrangements.
    - Access to provider's premises.
    - Obligations to implement and test business contingency plans.
    - Requirements to ensure continuity and quality of services.
5. **Register of Information (Art. 28(8-10)**
    - Maintain updated register information on all contractual arrangements.
    - Information to be submitted annually.
    - Harmonised templates (reporting).
6. **Exit Strategies & Transition Plans (Art. 28(7)**
    - Appropriate exit strategies.
    - Transition plans.
    - Considerations for disruptions.
    - Transfer functions to other providers / in-source.
7. **Ongoing Monitoring & Review**
    - Regularly monitor performance.
    - Review risk assessments.
    - Identify new risks.
    - Take appropriate measures.

Note on Penalties for Non-Compliance: Non-compliance with DORA can result in penalties of up to 2% of total worldwide annual turnover.

Legal basis: Regulation (EU) 2022/2554 (DORA), Commission Delegated Regulation (EU) 2024/1773 (contractual RTS).