DORA Impact Assessment Checklist

Are You Impacted by the Digital Operational Resilience Act (DORA)?

Industry Categories

Tick the boxes relevant to your business:

- Banks and Credit Institutions □
- Investment Firms □
- Insurance and Reinsurance Companies □
- Payment Institutions □
- Crypto Asset Service Providers □
- Alternative Investment Fund Managers □
- Market Infrastructures (e.g., Trading Venues, Central Counterparties) □
- ICT Third-Party Service Providers (e.g., Cloud, Data Centre, or Other Technology Providers to Financial Services) □

If you belong to one of the listed industries, your organization may be impacted by DORA.

Company Size

- Has your business been designated a critical ICT third-party service provider to financial entities, regardless of size? □
- Do you operate cross-border or provide services to EU financial entities? □

If you meet these criteria, DORA regulations may apply.

How Are UK Companies Affected?

Tick the boxes that apply to your business to assess the impact of DORA on UK-based companies:

1. **Do you provide financial or ICT services to EU-based financial entities or operate cross-border?**
    - Yes □
    - No □

2. Are you part of the supply chain for EU financial entities (e.g., banks, insurers, or crypto providers)?

- Yes ☐
- No ☐

3. Do you provide ICT services critical to operational resilience for financial entities in the EU?

- Yes ☐
- No ☐

4. Have you reviewed your compliance with DORA's requirements for ICT risk management, incident reporting, and operational resilience testing?

- Yes ☐
- No ☐

5. Are your IT security and risk management frameworks aligned with applicable requirements under UK financial regulations (e.g., FCA, PRA) and DORA?

- Yes ☐
- No ☐

6. Do you need to register with EU supervisory bodies (e.g., ESAs or NCA) for your operations in the EU?

- Yes ☐
- No ☐

If you answered "Yes" to any of the above questions, your UK business may need to take further action to align with DORA.

What Should You Do Now?

For EU Companies:

- Compliance with DORA:
  - Establish ICT risk management frameworks that comply with DORA.
  - Ensure effective incident reporting and operational resilience testing.
  - Maintain robust third-party risk management for ICT providers.

For UK Businesses:

- Assess your exposure to DORA if you operate cross-border or serve EU financial entities.
- Align your ICT risk management, incident reporting, and resilience testing with DORA requirements.
- Review your obligations under UK regulations, such as FCA or PRA, to check any overlaps with DORA compliance.
- Consider registering with relevant EU supervisory authorities if your services impact EU financial operations.

Disclaimer: The above checklist and recommendations are provided for informational purposes only and should not be construed as legal advice. Customers are strongly encouraged to seek advice from their legal advisors to ensure compliance with applicable laws and regulations