DORA Checkliste

Sind Sie vom Digital Operational Resilience Act (DORA) betroffen?

Branchen

Kreuzen Sie Ihre Branche an:

- Banken und Kreditinstitute ☐
- Investmentfirmen ☐
- Versicherungs- und Rückversicherungsunternehmen ☐
- Zahlungsinstitute ☐
- Krypto-Asset-Dienstleister ☐
- Verwalter alternativer Investmentfonds ☐
- Marktinfrastrukturen (z. B. Handelsplätze, zentrale Gegenparteien) ☐
- IKT-Drittanbieter (z. B. Cloud-, Rechenzentrums- oder andere Technologieanbieter für Finanzdienstleistungen) ☐

Wenn Ihr Unternehmen einer der genannten Branchen angehört, könnte es von DORA betroffen sein.

Unternehmensgröße

- Wurde Ihr Unternehmen als kritischer IKT-Drittanbieter für Finanzinstitute eingestuft, unabhängig von der Unternehmensgröße? ☐

Wenn Sie dieses Kriterium erfüllen, könnten die DORA-Vorschriften für Sie gelten.

Was sollten Sie jetzt tun?

Compliance mit DORA:

- Erstellen Sie IKT-Risikomanagement-Rahmenwerke, die den DORA-Vorgaben entsprechen.
- Stellen Sie eine effektive Vorfallberichterstattung und Tests der operationellen Resilienz sicher.
- Pflegen Sie ein robustes Risikomanagement für Drittanbieter im Bereich IKT.