Are You Ready for the Digital Operational Resilience Act?

The Digital Operational Resilience Act (DORA) is a new European regulation designed to strengthen digital resilience across the financial sector. With cyberattacks on European financial services rising by 200% between 2022 and 2023, DORA introduces a unified framework to enhance operational security and address gaps in digital defences.

Introduced under Regulation (EU) 2022/2554, DORA applies to financial institutions and ICT service providers operating within the EU. Even UK-based firms with European subsidiaries must comply, as DORA mandates improved risk management, incident reporting, resilience testing, and third-party risk oversight.

Timeline for Implementation

DORA came into effect on January 16th 2023, **with full compliance required by January 17th 2025.** Organisations must use this period to review and update their digital resilience strategies, avoiding fines for non-compliance starting in January 2025.

Key Requirements of DORA

1. **Governance and Control:** Strong internal ICT risk frameworks, such as ISO 27001, are essential.
2. **Incident Reporting:** Reporting major ICT-related incidents is mandatory.
3. **Resilience Testing:** Regular digital resilience testing, including penetration and recovery tests, is required.
4. **Third-Party Risk Management:** Critical suppliers must be evaluated rigorously.
5. **Information Sharing:** Strict guidelines on information sharing within financial entities.

DORA places accountability on management bodies, holding them directly responsible for ICT risk management. DORA also mandates annual reviews and testing of business continuity plans and includes an EU oversight framework for Critical Third-Party Service Providers (CTPPs).

T 0207 101 4861 | E info@ajollyconsulting.co.uk | www.ajollyconsulting.co.uk

The Urgency for Compliance

With the rise of AI-driven threats and politically motivated cyber-attacks, financial services are among the top three industries targeted in Europe. The increasing frequency and sophistication of these attacks make DORA compliance essential. Failure to adapt could lead to regulatory penalties, operational disruptions, legal challenges, and loss of customer trust.

How AJC Can Help

Partnering with third-party experts like AJC is a smart move for ensuring DORA compliance. Organisations must carefully assess their service providers to ensure they meet DORA's standards, particularly regarding data protection, incident reporting, and resilience testing. Regularly reviewing and testing your operational resilience measures, such as incident response plans, is crucial to minimising the impact of disruptions and staying compliant.

Take Action Today

With the compliance deadline fast approaching, now is the time to act. At AJC, we offer a tailored DORA Compliance Health Check to evaluate your current compliance status and provide actionable recommendations for improvement. We also assist with future compliance planning to ensure your organisation stays on track long after the initial assessment.

Let's Talk

Secure your organisation and prepare for the DORA compliance deadline by scheduling a **DORA Compliance Health Check** with our expert team. We're here to help protect your business and ensure long-term resilience.

Get in touch today and work with us to ensure your organisation is fully compliant before 17th January 2025

T 0207 101 4861 | E info@ajollyconsulting.co.uk | www.ajollyconsulting.co.uk