

DORA Compliance Blueprint: A Step-by-Step Guide to Strengthening Digital Operational Resilience

The Digital Operational Resilience Act (DORA) aims to enhance the digital resilience of financial entities within the European Union. To align with DORA's requirements, consider the following steps:

1. Assess Applicability:

- Determine if your organization falls under DORA's scope, which includes various financial entities and critical third-party service providers.

2. Establish an ICT Risk Management Framework:

- Develop a comprehensive framework to identify, assess, and manage information and communication technology (ICT) risks.
- Ensure the framework covers all stages of the ICT system lifecycle.

3. Implement Incident Reporting Procedures:

- Set up processes to detect, classify, and report major ICT-related incidents promptly to relevant authorities.
- Maintain records of incidents and responses for accountability.

4. Conduct Digital Operational Resilience Testing:

- Regularly test ICT systems to assess resilience against disruptions.
- Include threat-led penetration testing (TLPT) to simulate cyberattacks and evaluate defences.

5. Manage Third-Party ICT Risks:

- Assess and monitor risks associated with third-party ICT service providers.
- Ensure contractual agreements include provisions for risk management and compliance with DORA.

6. Facilitate Information Sharing:

- Engage in information-sharing arrangements with other financial entities to exchange cyber threat intelligence and best practices.

7. Prepare for Regulatory Oversight:

- Be ready for supervision by competent authorities, including potential audits and assessments.
- Maintain comprehensive documentation of compliance efforts and ICT risk management activities.

By following this blueprint, organizations can enhance their digital operational resilience and seek compliance with DORA's requirements.

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