waystone | Compliance Solutions

Navigating DORA compliance: A practical guide for SMEs

Conor Flynn June 19, 2024

To address the rising threats of cyber-attacks and digital disruptions in the financial sector, the European Union has introduced the Digital Operational Resilience Act (DORA). This regulation aims to ensure that financial institutions are equipped to effectively manage and mitigate digital risks.

For small and medium-sized investment managers, particularly those without extensive compliance resources, navigating these new regulations can seem daunting. This guide aims to demystify DORA, offering a clear and practical overview tailored to your needs.

The compliance deadline of 17 January 2025 is fast approaching. Organisations must act now to safeguard against evolving risks.

Does DORA apply to my fund?

If you answer yes to any of these questions, then DORA applies to you:

Q1: Are you an entity based in the EU?
Yes: DORA applies to your operations to ensure compliance with EU regulations on digital operational resilience.

Q2: Are you involved in one of these three areas of financial services: investment management, payment services, or insurance?
Yes: Your activities fall under the scope of DORA, requiring adherence to its guidelines.

Q3: Are you a UK, US or other non-EU entity with clients or funds in the EU?
Yes: Non-EU entities should ensure their compliance with DORA if they wish to service EU clients or managed EU funds.

Q4: Do you provide ICT services to financial institutions in the EU?
Yes: As a third-party service provider, you must ensure your practices meet DORA standards.

Q5: Do you manage digital assets or infrastructure that support financial services in the EU?
Yes: Your ICT frameworks and practices must align with DORA's requirements to mitigate digital risks.

What is DORA?

The EU's Digital Operational Resilience Act (DORA) has been in force since January 2023 and will be fully applicable from 17 January 2025. This regulation aims to ensure that all participants in the financial system have the necessary safeguards in place to mitigate cyber-attacks and other digital risks.

DORA will simultaneously affect five key operational framework areas:

1. ICT risk management:
Ensures the management body of the firm is responsible for identifying and managing relevant ICT risks, protecting the confidentiality, integrity and availability of digital assets.

2. ICT-Related incident management, classification and reporting:
Enhances regulatory reporting and transparency across financial entities, introducing standardised incident reporting and communication protocols.

3. Digital operational resilience testing:
Requires regular assessments of digital infrastructure to ensure it can withstand disruptions and recover effectively.

4. Information sharing arrangements:
Encourages the exchange of cyber threat information and intelligence among financial entities to improve detection and response to cyber threats.

5. Management of ICT third-party risk:
Imposes stricter regulations on outsourcing activities, requiring thorough due diligence and robust contractual arrangements with third-party service providers.

How to prepare for DORA

Here's how you can prepare for DORA compliance:

1. DORA readiness assessment:
Conduct a thorough assessment to evaluate your current compliance status. This involves performing personalised interviews and utilising detailed checklists to cover all relevant DORA aspects, ensuring a comprehensive evaluation of your systems and processes. Make sure to include aspects such as ICT risk management, incident reporting, operational resilience testing, information sharing and third-party risk management.

2. Detailed evaluation:
Using a comprehensive checklist, scrutinise your organisation's security framework against DORA-defined scope and metrics. This checklist should cover all critical areas including governance, risk management, operational resilience and third-party dependencies. Assess information security, along with legal requirements, to determine your current compliance status and pinpoint areas needing improvement.

3. Actionable reporting:
Develop a detailed report on the assessment results, covering compliance findings for each clause of DORA. This report should not only highlight areas of non-compliance but also prioritise them based on risk and impact. It should include necessary actions for technical, process and legal enhancements.

4. Personalised recommendations:
Based on the general report, define personalised DORA-compliance gaps and provide customised recommendations. These recommendations should address specific non-compliance areas, ensuring practical improvements and a smooth path toward full DORA compliance. Tailor these recommendations to the size and complexity of your organisation to ensure they are achievable and effective.

5. Consider outsourcing compliance:
For SMEs without extensive compliance resources, outsourcing the compliance function can be a viable option. Engaging external compliance experts or firms can provide the necessary expertise, support and resources to

ensure that your organisation meets all DORA requirements efficiently. This approach can also offer access to best practices and the latest compliance technologies.

By following these steps, you can proactively prepare for DORA compliance, ensuring that your operations are resilient and capable of withstanding digital risks and cyber-attacks.

How Waystone can help you comply with DORA

Waystone's Compliance Solutions team specialises in helping you stay ahead of the compliance gap. We offer tailored solutions to create and execute a customised DORA compliance plan, ensuring that your organisation meets all regulatory requirements efficiently and effectively.

DORA readiness assessment

Our experts will conduct a detailed assessment to evaluate your current compliance status and identify areas needing improvement. Through in-depth interviews and extensive checklists, we will thoroughly review your systems and processes against DORA's requirements, ensuring that all aspects of your operations are covered, from ICT risk management to incident reporting.

Heat map format

We provide a comprehensive heat map to outline the necessary work between now and the enforcement date, giving you a clear and actionable plan. This is a powerful visual tool that highlights compliance and non-compliance areas, categorised by risk and urgency.

The heat map helps by identifying critical areas through color-coded sections that pinpoint which parts of your operations need immediate attention. By prioritising tasks based on their risk impact and required timeline, you can ensure that high-risk areas are addressed first. As you implement compliance measures, the heat map is updated to reflect your progress, providing a clear visual representation of your journey towards full compliance.

Outcome-focused compliance

Waystone's approach ensures that your compliance efforts lead to tangible, positive outcomes, keeping you ahead of the compliance curve. Our focus is not just on meeting regulatory requirements but also on enhancing your overall operational resilience. We offer:

- **Personalised recommendations:** Tailored solutions that address your specific compliance gaps, ensuring practical and effective improvements.
- **Efficient personnel training:** We develop and implement training programs and workshops for your employees, ensuring they are well-versed in best practices for maintaining dependable, secure and resilient systems.
- **Continuous improvement**: We establish mechanisms for ongoing improvement and optimisation, such as feedback loops, performance monitoring and assessment tools. This ensures your organisation remains aligned with DORA principles over time.

Contact Waystone

For a personalised consultation and to start your DORA readiness journey, reach out to our compliance experts. We are committed to helping you navigate and comply with DORA regulations efficiently and effectively.

If you have any questions or would like to sign-up to receive our communications, please contact Conor Flynn or your usual Waystone representative via the below.

Contact Us →