Exploring DORA – a 5-step guide to compliance

---

1. Fund managers have until 1 January 2025 to comply with the DORA regulation

2. DORA emphasises the need for robust digital resilience plans to handle breaches, as demonstrated by recent high-profile cyber attacks

3. Below we outline the steps managers need to take to ensure they are compliant and meet the deadline.

With just six months to go until the deadline for fund managers to be DORA-compliant, Angel Ramon Martinez Bastida and Steve Pikett lay out an action plan to help you meet it amid growing digital threats to operations across the public and private sector.

The Digital Operational Resilience Act (DORA) is focused on how your organisation will fair if your defences are breached, and the processes and plans you need to have in place to continue business operations. IT Governance Europe reported that between November 2023 and April 2024, there were more than 2 billion known records breached, in 556 publicly disclosed incidents. Read the full report from 21 June 2024 here.

The UK's Cyber Security Breaches Survey of 2024 found that half of businesses and a third of charities in the UK reported a cyber breach or attack in the last 12

months. As the world around us digitises and becomes more virtually connected, a serious cyber-attack can have catastrophic impacts on people's lives and livelihoods.

A recent example includes the breach Ticketmaster's owner, Live Nation, confirmed had compromised over 560 million customers. The stolen data included names, addresses, phone numbers and partial credit card details from Ticketmaster users worldwide. This is just one incident, another is the recent NHS breach in which Russian hacking gang, Qilin, stole records including 300 million interactions between patients and the NHS – to see more look here World's Biggest Data Breaches & Hacks — Information is Beautiful.

What is the scope of DORA?

DORA harmonises the rules around operational resilience for the financial sector, applying to 20 different types of financial entities and ICT third-party service providers established in the EU, including authorised AIFMs (registered AIFMs are not in scope). Entities not headquartered in the EU might be exposed to DORA if part of their Group operates within the EU. It entered into force on 16 January 2023 and will apply as of 17 January 2025.

The regulation covers ICT risk management principles, digital operational resilience testing, reporting of major ICT-related incidents, and oversight of critical third-party providers.

There are real risks of enforcement for those who don't properly implement the requirements, however for many entities, much of the foundation will already be in place. So, a key part of the compliance roadmap will be identifying overlaps and gaps ahead of the January deadline.

5 key requirements to comply with DORA:

1. **ICT Risk Management Framework:** This requirement mandates financial entities to implement a robust ICT risk management framework, including a strategy for digital resilience. These should include clear roles and responsibilities for ICT-related functions, appropriate risk tolerance levels, and regular reviews of ICT policies, including Business Continuity and Disaster Recovery Plans.
2. **Incident Management and Reporting:** DORA requires a consistent incident reporting mechanism to reduce administrative burdens and

enhance supervisory effectiveness. Financial entities need to have procedures in place for managing and classifying ICT-related incidents and reporting them to the relevant authorities. Remediation plans and improvements made will also need to be reported on a regular basis.

3. **Digital Operational Resilience Testing:** Entities must conduct thorough testing of their ICT systems to ensure resilience. The testing should be sophisticated enough to identify important business services, set impact tolerances, and identify vulnerabilities. The sophistication of mapping and testing is expected to increase over time and will start with annual testing of all the ICT systems supporting critical functions.
4. **ICT Third-Party Risk Management:** This will need to be integrated into the general ICT risk management framework, and concentration risk from outsourcing and sub-outsourcing will need to be considered. The use of third-party ICT providers in third countries will be restricted and an information register will need to be maintained and reported to the authorities on a regular basis. The contracts with ICT parties will need to reflect the right from regulators to access and inspect the systems.
5. **Information and Intelligence Sharing:** DORA encourages the sharing of cyber threat intelligence and insight to improve digital operational resilience. Agreements on the exchange of information are expected from the entities, as well as the implementation of mechanisms to review and take action on the information shared by the authorities.

5 steps to take now to meet the compliance deadline:

1. **Identification and mapping:** This begins with a question about what is critical to your business, and what you want to protect – the functions, systems, processes and people, with all involvement mapped end-to-end. This is the best way to spot your weaknesses and put resilience plans in place.
2. **Governance, policies, and plans:** An inventory of existing policies around crisis comms, disaster management plans and business continuity are a good place to start as many will already be in place. To meet the requirements of DORA it is most useful to look for any gaps that might exist in your digital resilience policies and processes. You will need to ensure proper treatment of any ICT events and prompt communication to the authorities following the criteria set out in the regulation.
3. **Continuous training:** Members of the management body will be

required to regularly update their knowledge and skills regarding ICT risk. This will help in making informed decisions that align with your operational resilience objectives. Compulsory ICT security awareness programmes and resilience training within staff training schemes will need to be put in place too. These programmes will need to match the complexity of each employee's role.

4. **Third-party contracts:** The existing and new ICT contracts will need to be reviewed to ensure each party is aware of their roles and responsibilities in terms of regulatory reporting on breaches as well as how to manage the process when one is identified. Who will contact the regulator? How will the work to comply be split in terms of resources and cost? What are the time frames for identifying and reporting?
5. **Technical measures and testing:** You will need to implement advanced testing of ICT tools based on Threat-Led Penetration Testing ("TLPT", a controlled attempt to compromise the cyber resilience of an entity) and understand the skills required to run testing and conduct appropriate training. You will also need to put in place a first line of defence plan and test it regularly.

How can your outsourcing partner help?

There is no substitute for thorough due diligence and frequent checking of any outsourcing partner, but choosing a resilient outsourcing partner is key to ensure the robustness and safety of your operations and your business. With part of the Group being formally subject to DORA, Aztec is engaged in an ongoing journey to further increase its digital operational resilience and position itself as a robust and reliable partner.

To discuss DORA compliance or any of the points raised in this article, contact Angel Ramon or Steve directly.