The COMMENT

COMMENT

DORA: A PARADIGM SHIFT

Robert D Maddox and Tristan Lockwood at Debevoise & Plimpton assess new continuity requirements and suggest organisational and technical changes will be needed to comply

The EU Digital Operational Resilience Act (DORA) has the potential to be a game-changer for fund managers in Europe, for the first time imposing prescriptive technology-focused business continuity requirements. Coming into effect in January 2025, almost all large EU-regulated financial services entities – including alternative investment fund managers – are covered. Requirements include risk management, incident reporting, resilience testing and third-party contracting requirements. While many embody existing best practice, DORA will likely require organisational and technical changes at many firms to identify and plug compliance gaps against the new requirements.

Are you covered?

DORA – with limited exceptions – is one-size-fits-all. It applies to a wide-range of EU-regulated financial entities: banks, insurers, payment institutions, credit rating agencies, data reporting service providers, benchmark administrators, management companies, investment firms and managers of alternative investment funds.

For AIFMs, DORA carves out firms with leveraged assets less than €100m or unleveraged assets less than €500m with redemption rights exceeding five years. Some requirements are also softened for micro-enterprises, which employ fewer than 10 persons and have an annual turnover or annual balance sheet total less than €2m. While the one-size-fits-all approach presents challenges, DORA expressly incorporates proportionality as a key concept, potentially softening requirements that, on their face, could be extremely onerous for some firms.

Key requirements

ICT risk management: DORA requires a comprehensive ICT risk management framework, integrated into an overarching risk management system. This includes a requirement for a digital operational resilience strategy. DORA also expects firms to implement ICT systems and tools that are able to identify and mitigate ICT risks consistently and reliably, including IT asset lists, business continuity policies, disaster recovery plans and backup recovery procedures, among others. Even where firms have policies or procedures covering these in place already, they should review them against DORA's specific requirements (and yet to be released technical standards) to confirm compliance.

Incident reporting: Firms will be required to report all major ICT-related incidents to their existing financial regulator and notify individuals where an incident has an impact on their financial interests. Key aspects of the new regime still need to be settled though (such as reporting timeframes and format). Firms will also be required to inform customers about protective measures they should take in the event of a significant cyber threat, adding a further layer of complexity to the already interlocking web of notification obligations many firms face. DORA also requires various incident response and communication policies. Again, firms should assess whether any existing policies meet DORA's requirements, and supplement (or create) them if not.

Testing: DORA's new resilience-testing requirements generally reflect industry best practice: regular penetration testing, vulnerability and network security assessments, gap analyses and software solutions testing. Firms will also be required to conduct an annual operational resilience audit, which although another example of best practice being enshrined in law, entails a number of specific requirements. One big change is DORA's framework for cross-sector, regulator-overseen scenario-based testing. Given their risk profile though, it is unlikely that the private funds industry will take a leading role in any such exercises.

Contracting: Finally, DORA imposes minimum standards for all ICT-related contracts (and even tougher standards for contracts related to critical functions). These include prescribed mandatory contractual terms, mandatory risk assessments, due diligence and exit planning. Many larger firms may already have onboarding procedures in place that can be adjusted. Others may need to start from scratch.

Board requirements

Under DORA, boards bear ultimate responsibility for digital operational risk and are required to approve and regularly review the firm's risk management framework, incidents and the results of audits. Certain operational resilience tests will also need to be reported to the board, with lessons learned fed into remediation plans for board consideration and approval. Given the requirement for active engagement, DORA requires the board to keep up to date with sufficient knowledge and skills to understand and assess ICT risk and its impact on the operations, including through regular training. DORA also provides for individual liability for board members and, at the member state level, potential criminal penalties.

Tackling compliance

The volume of DORA's requirements means that firms will want to perform a gap analysis sooner rather than later to identify what work needs to be done. For most AIFMs, the gaps are likely to be larger than for bigger and more heavily regulated financial entities such as banks and payment service providers. DORA's emphasis on proportionality leaves potential scope for AIFMs, which typically have lower systemic risk profiles than many other financial entities, to adopt more narrowly tailored policies and procedures adapted to their specific business. Nevertheless, building compliance will still require collaboration across technology, legal, regulatory and compliance functions, as well with procurement stakeholders given DORA's wide scope.

Comparative perspectives

DORA is part of a continuing global trend toward greater operational resilience regulation in the financial sector, including private equity.

In the US, the Securities and Exchange Commission (SEC) in February 2022 released its 'Proposed Rule on Cybersecurity Risk Management for Investment Advisors, Registered Investment Companies and BDCs'. While far less prescriptive than DORA, the rules would impose extensive obligations on private equity firms to implement policies and procedures to deal with cyber risk, test those policies and procedures, and report incidents to the SEC. Following a lengthy comment period, the SEC announced its intention to finalise those rules in spring this year. Firms regulated in the US and EU may want to consider developing a framework that can meet both regulations' requirements.

Looking forward

Building DORA compliance may take time for many firms that, traditionally, have had less well-developed operational resilience frameworks than other types of regulated institutions. Even if AIFMs may be unlikely to be prime targets for DORA-related enforcement down the line, the new regime could provide low-hanging fruit for regulators when an incident occurs, and fertile ground for investor due diligence questionnaires in the future. ◆