POLICY

Exploring DORA

The EU's DORA regulation is just four months from taking effect, raising concerns about whether pension funds will be adequately prepared. One of the key challenges will be the scrutiny of third-party ICT vendors, along with the need for continuous testing. Lynn Strongin Dodds **reports**

The clock is truly ticking for European pension funds to get their houses in order for the Digital Operational Resilience Act (DORA). There are still a few loose ends to tie up, but schemes are advised to ramp up their efforts given the deadline is only four months away.

The task at hand should not be underestimated. As a new white paper by Broadridge in consultation with consultancy Firebrand notes, DORA, which comes into effect on 17 January 2025, is widely regarded as the most comprehensive and stringent regulation for operational resilience globally, requiring detailed self-assessment and planning. The rules also have extraterritorial reach, which means information technology and communications (ICT) third-party service providers within, as well as outside the European Union, will be in scope.

The paper says there is a growing sense that many firms remain far from ready, exposing themselves not only to operational resiliency risk, but also to regulatory failure. This could result in a fine as the national competent authorities can impose sanctions of up to 2 per cent of a firm's total annual worldwide turnover. Moreover, ICT third-party service providers that are designated as "critical" by the European Supervisory Authorities (ESAs) may face penalties of up to €5 million.

Recent comments by the Association for Financial Markets in Europe (AFME) underscore the urgency. It said the industry is under "severe pressure" to complete the necessary steps before January. Meanwhile, the European Cloud User Coalition (ECUC) in its feedback on DORA suggests that the implementation deadline should be extended to 17 January 2028 to allow for sufficient time for the industry to prepare.

An extension has not been granted for the 22,000 firms, including financial entities and ICT vendors, in the catchment area. However, there is a size limit to pension schemes. Those with 100 or more active and deferred members have to fully comply while those between 16 to 99 are subject to most of the legislation.

Goodwin financial services partner, Andrew Henderson, points out, however, that DORA is "not brand new" for financial sector entities in that much of it builds on

previous industry-specific guidelines to define requirements around consistent ICT risk management; comprehensive resilience testing capabilities, including threat-led penetration testing and third-party risk management. "It is an evolution, but it not created from scratch," he adds. "DORA codified and hardwires what has been guidance."

THE PURPOSE OF DORA

DORA aims to create a more coherent and comprehensive framework from an often disjointed, patchwork set of rules scattered across different sectors and EU countries. The hope is that this will bolster the IT defences of the region's financial service firms in the event of a serious disruption, such as a cyber-attack, by focusing on five key areas. These include ICT risk management, ICT-related incidents, digital operational resilience testing, third party risk and information sharing.

"THE FOCUS SHOULD BE ON THE EXISTING STRUCTURE IN PLACE, WHAT IS REQUIRED UNDER DORA, WHAT NEEDS TO BE DONE, THE TRAINING THAT WILL BE REQUIRED AND WHO WILL BE RESPONSIBLE FOR THIS"

DORA is also part of a wider global legislative agenda that pension funds need to be cognisant of even if they are not directly impacted by it. This includes the Critical Entities Resilience Act (CER), Network and Information Systems Security 2 Directive (NISD2) and Data Governance Act. Last year also saw an agreement reached on the Cyber Resilience Act, the first set of global cybersecurity rules for digital and connected products that are designed, developed, produced and made available on the EU market.

Although the devil is always in the detail, some issues remain unresolved. Market participants had hoped the ESAs would have added more clarity around vendor subcontracting in the second batch of regulatory technical standards published in July. However, there was no further information or explanation as to why guidance was delayed. Instead, they said it would be published in "due course."

PREPARATION IS KEY

In the meantime, the Broadridge

report recommends pension funds should devise a blueprint and undergo a detailed health check to assess the criticality of its systems and services, including a review of how closely aligned its existing ICT governance frameworks are with DORA's requirements. Attention should also be paid to identifying important business services that, if disrupted, could cause a negative impact throughout the firm and market. In addition, the scheme needs to ensure that the right people, processes, technology, facilities and information, including those of suppliers, are in place.

The first step though, according to Mason Hayes & Curran partner and head of pensions, Stephen Gillick, is to conduct a gap analysis to identify deficiencies in existing practices. "The focus should be on the existing structure in place, what is required under DORA, what needs to be done, the training that will be required and who will be responsible for this," he adds. "There were a lot of lessons learnt in getting ready for IORP II that can be applied here but there is a recognition that many of the larger schemes already have process in place and are familiar with the issues but that is not the case with the smaller ones."

As PensionDanmark chief digital risk officer, Janus Friis Bindslev, says: "PensionDanmark has worked with critical third-party vendor risk through several years, so in that sense it is not new. There are still open questions around the detailed requirements on vendors and their supply chains, as not all of the regulatory standards have been published yet. But as a pension fund we want to be as efficient as possible in managing this risk and not wait until everything is finalised."

One of the biggest issues for many pension funds will be to examine their third-party vendor relationships that have not come under such intense scrutiny in the past. This comprises greater due diligence, such as reviewing contracts, as well as developing a monitoring and reporting system for third-party risks. It also entails ongoing monitoring and regular assessments of these providers.

"DORA is multi layered and a much more granular piece of regulation," says Sidley partner and global co-chair of its privacy and cybersecurity practice, William Long. "It requires a holistic and comprehensive review of policies, procedures as well as contractual arrangements. This does not just cover the third-party service provider but also their subcontractors. This is not just a case of updating but also amending a large number of contracts, which is a huge exercise."

Henderson also expects to see an increase in contract negotiations and a tightening of language. He believes that the operational resilience and risk of third-party providers will be held to a much higher standard than before.

Testing is also seen as a challenge as the RTS are requiring financial service firms to demonstrate the governance of their critical services via regular monitoring, consistent metrics and tolerance setting for each critical service. They will have to establish procedures that enable a variety of testing and techniques including vulnerability scanning, penetration testing, red teaming and tabletop exercises. This may be a new practice for even the bigger schemes.

The first, which is expected to be done on a regular basis, identifies cracks in the system as well as detecting potential exploitation, while the second builds upon the vulnerability scan and will typically be conducted annually.

Red teaming, an increasingly popular application, looks at the attackers in the simulation, employing tactics, techniques, and procedures (TTPs) that hackers would use. Last but not least, tabletop exercises are scenarios whereby existing procedures and processes are examined.

Although implementing the right resources and technology is crucial, it is only one part of the equation. Management buy in is critical in that they need to ensure that the organisation is working in tandem to meet the impending deadline.

"One of the biggest challenges is under appreciation at board level that proactive risk reduction can be achieved by DORA," says Thomas Murray director GRC, cyber risk, Shreeji Doshi. "An interesting perspective, DORA requires that the board puts appropriate governance structures to enable risk appropriate spending as there are multiple risk areas competing for budget spend."