Are you really ready for the DORA environment?

Demi Derem, SVP International Investor Communication Solutions at Broadridge, looks at the six factors that will determine compliance in proxy services

Our digital world is complex, characterised by a multitude of interconnected systems and data that is stored — and widely shared — online.

It is well known that cyberthreats are becoming more sophisticated, posing significant risks to financial stability and security.

Outages too, such as the 2024 CrowdStrike IT issue affecting millions of devices around the world, is one recent example of a 'left hook' that caught many by surprise.

Against this backdrop, the EU's Digital Operational Resilience Act (DORA) has entered into force, with in-scope firms — including banks and investment firms — required to be fully compliant from 17 January 2025. Fintechs must ensure that they are well-positioned to help banks and investment firms comply.

DORA establishes a clearer foundation for security and operational resilience in the financial services sector, while also aligning with other EU measures on cybersecurity and data. It reflects the thinking in other markets around the world, with regulators increasingly demanding that financial institutions bolster their operational resilience, and that of their supply chains.

An amplification of responsibility

DORA is structured around five pillars, covering governance, resiliency, incident management, information sharing, and reporting.

The common thread is the protection of data as it passes through both a financial institution and the ecosystem around it. This is particularly pertinent in the proxy world, and the automated solutions that power proxy voting across global markets. Stakeholders must now pay much closer attention to where the data is going, and ensure they are carrying out detailed information security reviews.

Resiliency in the past has tended to be quite inward looking, with firms focusing on ensuring their own house is in order. DORA has shifted the dial, and mandates firms to extend this externally across service providers utilised.

Beyond ensuring their own compliance, asset managers must also assess and make sure that their service providers can help them comply with DORA. Their responsibility does not end with their primary vendors' services; they also need to be comfortable that any subcontractors who are providing critical service can also help the asset managers to comply. Failure to do so can result in sanctions of an administrative, financial, or even criminal nature — and the asset manager is always on the hook.

Providing the right questions to ask

If you are providing services to an asset manager, it is no longer just a case of ensuring that you are fully compliant and fit for purpose; the buyer needs to be sure that any supplier and any subcontractors of critical services can help you comply with DORA.

Digital Resilience

Here are the six key information requests you should be cascading urgently. If your suppliers can provide positive answers to all of the below, then you are likely to be DORA compliant. If there are gaps, then there are real to-dos for your firm:

- **Supply chain resiliency:** You will need evidence that each of your vendors is operationally resilient. If they become insolvent, their technology drops, or if they suffer a data breach, then do you or they have a comprehensive and resilient plan in place?

- **Data security standards:** You need to check out their encryption standards for data at rest and in transit for the services they provide, including the procedures in place to address any data leakages. Your vendors' data security standards should be robust and reflected throughout the supply chain they use for your critical services.

- **Critical services restoration:** You and your vendors must evidence recovery procedures for any outsourced services, detailing the steps to recover from major incidents. Information should include timelines regarding the resumption of normal operations after an IT outage and/or cyberattack. If it is a regulated activity and a time-critical regulated function, like proxy, then what is their back up? How will they stay online and ensure that they can help you comply? Ideally, they should have appropriate disaster recovery centres, so if something happens in one location, they can be fully live in another.

- **Detection and monitoring:** You will also need evidence of effective cyber intrusion detection and how they monitor how cybercriminals are attempting to access their systems and data. Appropriate evidence includes penetration tests conducted by the vendor and any third parties they use to provide critical services. The completeness of everyone's cybersecurity strategies should be consistent across the supply chain in order to protect the asset manager.

"DORA compliance is not a 'nice-to-have'; it is mandatory and it is now business as usual"

- **Information security:** You must obtain confirmation from your service providers that they comply with appropriate information security standards, including details of policies they are adhering to and how residual information security risks are being managed and monitored. This applies to all third parties providing critical services throughout the supply chain.

- **Critical services full ecosystem compliance:** Finally, you must request confirmation from your providers that they are able to assist you in your compliance of DORA, and if there are gaps in their ecosystem which need to be closed, what they are doing to remediate the gaps.

DORA compliance is not a 'nice-to-have'; it is mandatory and it is now business as usual. It is also worth noting that Broadridge's 2024 Digital Transformation & Next-Gen Technology Study highlighted that cybersecurity is the top concern of C-suite technology executives, usurping timely delivery of projects and sticking to budgets.

If you are still unclear about your firm's DORA compliance obligations, I would strongly advise a conversation with your compliance and product leaders. Further information on DORA is also available in our whitepaper on the topic.