Shutterstock Royalty-free stock illustration ID: 1170542227 Stock market or forex trading graph in graphic to symbolise financial services industry

May 12, 2021 12:55 BST

Spotlight on the EU's Digital Operational Resilience Act (DORA)

Following our spotlight on the UK's new operational resilience regulation proposed by the Bank of England,

Simon Fieldhouse, global managing director – Software Resilience now focuses on the EU Commission's own approach to operational resilience within financial services with the Digital Operational Resilience Act (DORA).

In our ‘Spotlight on’ series, we explore what this will mean for the sector and the actions affected businesses should take.

What does the regulation say?

DORA is a draft regulation published by the European Commission. It is part of the Commission's wider Digital Finance Strategy which aims to support growth in digital finance and manage risk.

It’s aimed at financial entities regulated at EU level which includes everything from credit and payment institutions to credit rating agencies and crowdfunding service providers.

The regulation covers a range of IT-related requirements, encompassing risk management, incident reporting, third-party risk and information sharing.

The demands around third-party technology risk are quite significant. The regulation introduces key requirements to be included in financial entities’ contracts governing the relationship with third parties. These include provisions on accessibility, availability, integrity, security, as well as guarantees for access, recovery and return in case of failure of third-party service providers. ‘Exit strategies’ should be determined and tested too.

Why has the regulation been proposed?

DORA comes as businesses across the financial sector are using more and more software to drive efficiencies, boost productivity and enhance user experience – and this has intensified over the pandemic. But all of this creates more complex supply chains, and in turns increases the risk profile of an organisation.

Ultimately this regulation responds to these changes and is about protecting the sector, ensuring there is proper operational resilience baked into the EU’s entire financial services industry. The impact of a single supplier failing could have a huge effect on business continuity – and the European Commission wants to force organisations to have the appropriate processes in place to anticipate, withstand and respond to disruption.

What should financial services businesses do now?

The regulation is due to come into effect around 2023, and while this seems a long way off, there will no doubt be changes to come and there is plenty that financial leaders can do to prepare now.

When it comes to third-party risk, the elements set out in DORA – relating to accessibility, availability, integrity, security and access to data in the case of insolvency, resolution or discontinuation of business operations by service provider – are the right areas to focus on. Escrow agreements and verification tests with all third-party software suppliers solve this issue. And 'exit strategies' – which DORA mandates – can easily be tested with your escrow provider.

Third-party risk is an area financial regulators across the globe are turning their focus to. Finding a way to mitigate this risk holistically will be key for financial organisations. In the UK, the Prudential Regulation Authority (PRA) has been clear that software escrow is a practical solution, and it stands to reason that that's the case with DORA too – given their similarities.

Overall, the European Commission is aiming to boost the resilience of the financial services sector in the face of greater adoption of cloud technologies. This is about promoting growth and innovation in a sustainable way – and there's nothing stopping businesses getting ahead of the curve and putting the right measures in place now.

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 14,000 customers to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience, and investment in research and innovation, it is best placed to help organisations assess, develop and manage their cyber resilience posture.

With circa 2,000 colleagues in 12 countries, NCC Group has a significant market presence in North America, Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

Contacts

NCC Group Press Office
Press Contact
All media enquires relating to NCC Group plc
press@nccgroup.com
+44 7824 412 405
+44 7976 234 970