EUROFI VIEWS MAGAZINE - ZAGREB APRIL 2020

Simon Chard

Partner, Operational Resilience Lead, PwC

Standardised regulatory requirements can improve operational resilience

Everyone is talking about operational resilience. With a fast moving COVID-19 that may become the ultimate stress test, right in the middle of regulatory consultations across Europe, it's the key topic for firms. There is no shortage of policy areas to focus on to make both individual firms and the wider financial system more resilient. We covered a number of them in depth in our report "Operational Resilience: Time to Act" with theCityUK. In this article, I'd like to focus on four areas identified by the European Commission in their consultation: ICT and security risk management and incident reporting requirements, digital operational resilience testing and third party oversight.

The current state of ICT and security management requirements in Europe is inconsistent across sectors. While I don't believe anyone needs to be convinced that improved, consistent standards for risk and resilience across Europe would lead to an uplift in practices, let's talk benefits. Operational resilience is an outcome, not a process, function or methodology. So benefits must be evident from any initiative taken. For firms, having one standard means a level playing field in Europe, and clarity about what is expected for service chains which cross borders into different regulatory territories. For customers, improved management of risks means more reliable services and improved trust in financial institutions.

It goes without saying that even with the best risk management in the world, failure is inevitable. Industry-recognised standards on the timeliness and nature of reported incidents would enable customers to make decisions based on the relative resilience of firms. Increased consistency and transparency of reporting can also accelerate industry-wide detection of emerging systemic risks and help regulators and firms in their responses.

This understanding of emerging risks should be used to drive digital operational resilience testing. While almost all firms adhere to an operational testing regime, there is again currently no standardised framework. While such a framework may increase costs, if applied with appropriate proportionality, it could not only give firms more confidence in their own ICT and security estate but also that of other firms in their supply chain. For customers, improved and consistent testing will lead to greater confidence in the security and privacy of their assets.

Thinking about supply chains leads us to the final policy area: third party oversight. Third party failure is one of the most common causes of outages, so how well third parties are managed can clearly have a critical impact on the resilience of financial firms and markets. A common framework to manage third parties would not only reduce systemic risk by uplifting standards but also allow firms to leverage this framework to demand more of their suppliers via increased audit rights and participation in scenario stress tests.

Harmonisation of requirements across sectors in Europe can clearly be beneficial not just for customers but for firms and markets. While Brexit may create challenges for European harmonisation, we shouldn't lose sight of the fact that financial services routinely cross borders and therefore greater standardisation with shared global norms will surely be a good thing. ●