EVERSHEDS SUTHERLAND

# Flash update

## Operational Resilience: the clock has started; time to act is now

### Summary

Yesterday morning, Lyndon Nelson (Deputy CEO, PRA) and Suman Ziaullah (Head of Department for Technology, Resilience and Cyber Specialists, FCA) delivered key note addresses at City & Financial's 8th Operational Resilience and Cyber Security Summit. Both regulators reiterated and built upon the messages in Lyndon's previous speech on 5 May 2021, which was the focus of our last Flash Update on operational resilience. The key points arising from today's speeches are as follows:

- Inadequacies in basic cyber hygiene, such as patch management and storage of user account information, are at the heart of 80% of incidents.
- To date, the regulatory focus has been on the 40 largest firms which pose a systemic risk to the UK financial services market. The testing used to assess a firm's resilience has also largely comprised penetration testing.
- The regulators are now developing their testing tookits to: (i) broaden the scope of firms covered by the testing regime; (ii) extend coverage to include focus on a firm's response to an incident and its ability to recover in the timeframe stipulated for a severe but plausible scenario; and (iii) increase the frequency of testing.
- Although changes were made to the final policy statement on operational resilience to provide firms with more time and flexibility, firms should take steps as soon as reasonably practicable to implement the requirements.
- The regulators' focus in the period to 31 March 2022 will be on ensuring that firms are making adequate progress in identifying their important business services, setting impact tolerances and identifying vulnerabilities. Firms will also be expected to comply with broader aspects of the operational resilience requirements, such as ensuring that self-assessments are up-to-date and available upon request.
- In the subsequent transition period up to 31 March 2025, the focus will shift to assessing firms' abilities to remain within the impact tolerances they have set. Thereafter, the expectation will be that firms will consistently remain within their impact tolerances.
- Finally, in the next few weeks, the Cross Market Operational Resilience Group will be publishing a good practice guide to promote and support consistency in how firms communicate to internal and external stakeholders regarding incidents.

### Impact and actions

Now is the time to take lessons learned from the pandemic and bolster existing resilience plans. In the event of a future significant disruption event, we expect the regulators will be highly critical of a firm if it is unable to demonstrate how it has incorporated those lessons into its operational resilience framework.

Firms should also already be working on their self-assessments to ensure that they are in place by the regulatory deadline of 31 March 2022. Although there is no prescribed format, the regulator has emphasised that they must be clear, well-structured and accurate. This means that Boards and senior management must be able to evidence that they have scrutinised the contents and satisfied themselves that the underlying rationale for the identified important business services and ascribed impact tolerances is reasonable. Following 31 March 2022, self-assessments will need to be reviewed and updated on a regular basis.

### RAG rating

**Immediate impact**

## Links

Flash Update – Building Operational Resilience: The PRA view

Cyber Risk: 2015 to 2027 and the Penrose steps - speech by Lyndon Nelson

## Contact

**Hayley Astles**
*Senior Associate*

**T:** +44 20 7919 4751
**M:** +44 746 912 4989
hayleyastles@eversheds-sutherland.com

**eversheds-sutherland.com**