Chapter 15A

Operational resilience

15A.5 Scenario testing

Testing plan

15A.5.1 R A *firm* must develop and keep up to date a testing plan that appropriately details how it will gain assurance that it can remain within the *impact tolerances* for each of its *important business services*.

15A.5.2 G *Firms* should ensure that the testing plan takes account of a number of factors, including but not limited to:

(1) the type of scenario testing undertaken. For example, whether it is paper based, simulations or through the use of live-systems;

(2) the scenarios which the *firm* expects to be able to remain within their *impact tolerances* and which ones they may not;

(3) the frequency of the testing;

(4) the number of *important business services* tested;

(5) the availability and integrity of supporting assets;

(6) how the *firm* would communicate with internal and external stakeholders effectively to reduce the harm caused by operational disruptions.

Testing

15A.5.3 R A *firm* must carry out scenario testing, to assess its ability to remain within its *impact tolerance* for each of its *important business services* in the event of a severe but plausible disruption of its operations.

15A.5.4 R In carrying out the scenario testing, a *firm* must identify an appropriate range of adverse circumstances of varying nature, severity and duration relevant to its business and risk profile and consider the risks to the delivery of the *firm's important business services* in those circumstances.

15A.5.5 G Where a *firm* relies on a third party for the delivery of its *important business services*, we would expect the *firm* to work with the third party to ensure the validity of the *firm's* scenario testing under SYSC 15A.5.3R. To the extent that the *firm* relies on the third party to carry out testing of the services provided by the third party to or on behalf of the *firm*, the *firm* should ensure the suitability of the methodologies, scenarios and considerations

adopted by the third party in carrying out testing. The *firm* is ultimately responsible for the quality and accuracy of any testing carried out, whether by the *firm* or by a third party.

15A.5.6 G In carrying out the scenario testing, a *firm* should, among other things, consider the following scenarios:

(1) corruption, deletion or manipulation of data critical to the delivery of its *important business services*;

(2) unavailability of facilities or key people;

(3) unavailability of third party services, which are critical to the delivery of its *important business services*;

(4) disruption to other market participants, where applicable; and

(5) loss or reduced provision of technology underpinning the delivery of *important business services*.

15A.5.7 R A *firm* must carry out the scenario testing:

(1) if there is a material change to the *firm's* business, the *important business services* identified in accordance with ■ SYSC 15A.2.1R or impact tolerances set in accordance with ■ SYSC 15A.2.5R;

(2) following improvements made by the *firm* in response to a previous test; and

(3) in any event, on a regular basis.

Lessons learned

15A.5.8 R A *firm* must, following scenario testing or, in the event of an operational disruption, after such event, conduct a lessons learned exercise that allows the *firm* to identify weaknesses and take action to improve its ability to effectively respond and recover from future disruptions.

15A.5.9 R Following the lessons learned exercise, a *firm* must make necessary improvements to address weaknesses identified to ensure that it can remain within its *impact tolerances* in accordance with ■ SYSC 15A.2.9R.