

Senior arrangements, Systems and Controls

Chapter 15A

Operational resilience

15A.2 **Operational resilience
requirements**

Important business services

- 15A.2.1** **R** A *firm* must identify its *important business services*.
- 15A.2.2** **R** A *firm* must keep its compliance with **■** SYSC 15A.2.1R under review and, in particular, consider its compliance in the following circumstances:
- (1) if there is a material change to the *firm's* business or the market in which it operates; and
 - (2) in any event, no later than 1 year after it last carried out the relevant assessment.
- 15A.2.3** **G** In the course of identifying its *important business services* under **■** SYSC 15A.2.1R, a *firm* should treat each distinct relevant service separately, and should not identify a collection of services as a single *important business service*.
- 15A.2.4** **G** The factors that a *firm* should consider when identifying its *important business services* include, but are not limited to:
- (1) the nature of the *client* base, including any vulnerabilities that would make the *person* more susceptible to harm from a disruption;
 - (2) the ability of *clients* to obtain the service from other providers (substitutability, availability and accessibility);
 - (3) the time criticality for *clients* receiving the service;
 - (4) the number of *clients* to whom the service is provided;
 - (5) the sensitivity of data held;
 - (6) potential to inhibit the functioning of the *UK financial system*;
 - (7) the *firm's* potential to impact the soundness, stability or resilience of the *UK financial system*;
 - (8) the possible impact on the *firm's* financial position and potential to threaten the *firm's* viability where this could harm the *firm's clients* or

pose a risk to the soundness, stability or resilience of the *UK financial system* or the orderly operation of the financial markets;

- (9) the potential to cause reputational damage to the *firm*, where this could harm the *firm's clients* or pose a risk to the soundness, stability or resilience of the *UK financial system* or the orderly operation of the financial markets;
- (10) whether disruption to the services could amount to a breach of a legal or regulatory obligation;
- (11) the level of inherent conduct and market risk;
- (12) the potential to cause knock-on effects for other market participants, particularly those that provide financial market infrastructure or critical national infrastructure; and
- (13) the importance of that service to the *UK financial system*, which may include market share, *client* concentration and sensitive *clients* (for example, governments or pension funds).

Impact tolerances

15A.2.5 **R** A *firm* must, for each of its *important business services*, set an *impact tolerance*.

15A.2.6 **R** A *firm* must keep its compliance with **■ SYSC 15A.2.5R** under review and, in particular, consider its compliance in the following circumstances:

- (1) if there is a material change to the *firm's* business or the market in which it operates; and
- (2) in any event, no later than 1 year after it last carried out the relevant assessment.

15A.2.7 **G** The factors that a *firm* should consider when setting its *impact tolerance* include, but are not limited to:

- (1) the nature of the *client* base, including any vulnerabilities that would make the *person* more susceptible to harm from a disruption;
- (2) the number of *clients* that may be adversely impacted and the nature of the impact;
- (3) the potential financial loss to *clients*;
- (4) the potential financial loss to the *firm* where this could harm the *firm's clients* or pose a risk to the soundness, stability or resilience of the *UK financial system* or the orderly operation of the financial markets;
- (5) the potential level of reputational damage to the *firm* where this could harm the *firm's clients* or pose a risk to the soundness, stability or resilience of the *UK financial system* or the orderly operation of the financial markets;

- (6) the potential impact on market or consumer confidence;
- (7) potential spread of risks to their other business services, other *firms* or the *UK financial system*;
- (8) the potential loss of functionality or access for *clients*;
- (9) any potential loss of confidentiality, integrity or availability of data;
- (10) the potential aggregate impact of disruptions to multiple *important business services*, in particular where such services rely on common operational resources as identified by the *firm's* mapping exercise under ■ SYSC 15A.4.1R.

15A.2.8 **G** When setting its *impact tolerance*, a *firm* should take account of the fluctuations in demand for its *important business service* at different times of the day and throughout the year in order to ensure that its *impact tolerance* reflects these fluctuations and is appropriate in light of the peak demand for the *important business service*.

15A.2.9 **R** A *firm* must ensure it can remain within its *impact tolerance* for each *important business service* in the event of a severe but plausible disruption to its operations.

15A.2.10 **G** While under ■ SYSC 15A.2.9R a *firm* must ensure it is able to remain within its *impact tolerance*, it should generally not do so if this would put the *firm* in breach of another regulatory obligation, conflict with the proper exercise of a discretion granted to it under any *rule* or regulation, or result in increased risk of harm to its *clients* or the soundness, stability or resilience of the *UK financial system* or the orderly operation of the financial markets. Under certain circumstances, a *firm* may wish to resume a degraded service. This is usually only appropriate if having regard to the interest of the *firm's clients*, the soundness, stability and resilience of the *UK financial system* and the orderly operation of the financial markets, the benefits of resuming a degraded service outweigh the negatives of keeping the service unavailable until the issues have been fully remediated and the service is able to be fully restored to its pre-disruption levels.

15A.2.11 **G** Under *Principle 11* (Relations with regulators), the *FCA* expects to be notified of any failure by a *firm* to meet an *impact tolerance*.

15A.2.12 **G** When setting *impact tolerances* under ■ SYSC 15A.2.5R a *payment services provider* should have regard to its obligations under the *EBA Guidelines* on ICT and security risk management.

15A.2.13 **G** *Payment service providers* should have regard to the *impact tolerance* set under ■ SYSC 15A.2.5R when complying with the *EBA Guidelines* on ICT and security risk management. In particular, they should, as part of their continuity planning and testing, consider their ability to remain within their *impact tolerance* through a range of severe but plausible disruption scenarios.

15A