

**Senior arrangements, Systems and Controls**

## Chapter 15A

# Operational resilience



## 15A.1 Application

### Application

---

- 15A.1.1** **R** This chapter applies to:
- (1) a *firm* that is:
    - (a) an *enhanced scope SMCR firm*;
    - (b) a *bank*;
    - (c) a *designated investment firm*;
    - (d) a *building society*;
    - (e) a *Solvency II firm*,
  - (2) a *UK RIE*;
  - (3) an *electronic money institution*, a *payment institution* or a *registered account information service provider*; and
  - (4) a *consolidated tape provider*.
- 15A.1.2** **R** In this chapter, a reference to a *firm* includes a *UK RIE*, an *electronic money institution*, a *payment institution*, a *registered account information service provider* and a *consolidated tape provider*.
- 15A.1.3** **R** This chapter does not apply to a *TP firm*, a *TA PI firm*, a *TA RAISP firm* or a *TA EMI firm*.
- 15A.1.4** **R** This chapter does not apply to a *firm* which has its registered office (or, if it has no registered office, its head office) outside the *United Kingdom*.
- 15A.1.5** **R** In this chapter, a reference to a *client* in relation to a *UK RIE* includes a *person* who is entitled, under an arrangement or agreement between them and that *UK RIE*, to use the *UK RIE's facilities*.
- 15A.1.5A** **R** This chapter applies in relation to a *consolidated tape provider* as if a reference to a *client* includes a *person* who purchases a *consolidated tape for bonds* from:

- (a) a *consolidated tape provider*; or
- (b) a *data vendor*.
- 15A.1.6** **R** In this chapter, a reference to a *client* in relation to a *firm* carrying on the activity of *managing a UK UCITS* or *managing an AIF* includes:
- (1) a *unitholder*; and
- (2) an investor in an *AIF*.
- 15A.1.7** **R** The requirements in this chapter apply with respect to:
- (1) *regulated activities*;
- (2) activities that constitute *dealing in investments as principal*, disregarding the exclusion in article 15 of the *Regulated Activities Order* (Absence of holding out etc.);
- (3) *ancillary activities*;
- (4) in relation to *MiFID* or *equivalent third country business, ancillary services*;
- (5) *collective portfolio management*;
- (6) the provision of *payment services* and the issuance of *electronic money*, and activities connected to the provision of *payment services* and to the issuing of *electronic money* (whether or not the activity of issuing *electronic money* is specified in article 9B of the *Regulated Activities Order*);
- (7) any other *unregulated activities*, but only in a *prudential context*; and
- (8) *data reporting services* provided by a *consolidated tape provider*.
- 15A.1.8** **R** Notwithstanding **SYSC 15A.1.7R**, where the requirements in this chapter apply to a *firm* only as a result of **SYSC 15A.1.1R(3)**, the requirements only apply to the provision of *payment services* and the issuance of *electronic money* by the *firm*, and activities connected to the provision of *payment services* and to the issuing of *electronic money* (whether or not the activity of issuing *electronic money* is specified in article 9B of the *Regulated Activities Order*).
- 15A.1.9** **R** There is no territorial limitation on the application of this chapter.

## 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



**15A.3 Strategies, processes and  
systems**

- 15A.3.1** **R** *A firm must have in place sound, effective and comprehensive strategies, processes and systems to enable it to comply with its obligations under this chapter.*
  
- 15A.3.2** **R** *The strategies, processes and systems required under ■ SYSC 15A.3.1R must be comprehensive and proportionate to the nature, scale and complexity of the firm's activities.*

 15A.4 Mapping

- 15A.4.1** **R** A *firm* must identify and document the people, processes, technology, facilities and information necessary to deliver each of its *important business services*. This must be sufficient to allow the *firm* to identify vulnerabilities and remedy these as appropriate.
- 15A.4.2** **G** Where a *firm* relies on a third party for the delivery of an *important business service*, we would expect the *firm* to have sufficient understanding of the people, processes, technology, facilities, and information that support the provision by the third party of its services to or on behalf of the *firm* so as to allow the *firm* to comply with its obligations under ■ SYSC 15A.4.1R.
- 15A.4.3** **R** A *firm* must keep its compliance with ■ SYSC 15A.4.1R under review and, in particular, review its compliance in the following circumstances:
- (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; and
  - (2) in any event, no later than 1 year after it last carried out the relevant assessment.





## 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.

## 15A.6 Self-assessment and lessons learned exercise documentation

- 15A.6.1** **R** A *firm* must make, and keep up to date, a written record of its assessment of its compliance with the requirements in this chapter, including, but not limited to, a written record of:
- (1) *important business services* identified by the *firm* and the justification for the determination made;
  - (2) the *firm's impact tolerances* and the justification for the level at which they have been set by the *firm*;
  - (3) the *firm's* approach to mapping under ■ SYSC 15A.4.1R, including how the *firm* has used mapping to:
    - (a) identify the people, processes, technology, facilities and information necessary to deliver each of its *important business services*;
    - (b) identify vulnerabilities; and
    - (c) support scenario testing;
  - (4) the *firm's* testing plan and a justification for the plan adopted;
  - (5) details of the scenario testing carried out as part of its obligations under ■ SYSC 15A.5, including a description and justification of the assumptions made in relation to scenario design and any identified risks to the *firm's* ability to meet its *impact tolerances*;
  - (6) any lessons learned exercise conducted under ■ SYSC 15A.5.8R;
  - (7) an identification of the vulnerabilities that threaten the *firm's* ability to deliver its *important business services* within the *impact tolerances* set, including the actions taken or planned and justifications for their completion time;
  - (8) its communication strategy under ■ SYSC 15A.8.1R and an explanation of how it will enable it to reduce the anticipated harm caused by operational disruptions; and
  - (9) the methodologies used to undertake the above activities.

- 15A.6.2** **R** A *firm* must retain each version of the records referred to in ■ SYSC 15A.6.1R for at least 6 years and, on request, provide these to the FCA.



## **15A.7 Governance**

**15A.7.1**

**R**

A *firm* must ensure that its *governing body* approves and regularly reviews the written records required under ■ SYSC 15A.6 (Self-assessment and lessons learned exercise documentation).

**15A**



## 15A.8 Communications

- 15A.8.1** **R** A *firm* must maintain an internal and external communication strategy to act quickly and effectively to reduce the anticipated harm caused by operational disruptions.
- 15A.8.2** **G** As part of a *firm's* communications strategy, the *FCA* expects the *firm* to:
- (1) consider, in advance of a disruption, how it would provide important warnings or advice quickly to *clients* and other stakeholders, including where there is no direct line of communication;
  - (2) use effective communication to gather information about the cause, extent, and impact of operational incidents; and
  - (3) ensure that their choice of communication method takes account of the circumstances, needs and vulnerabilities of their *clients* and other stakeholders.
- 15A.8.3** **R** A *firm* must provide clear, timely and relevant communications to stakeholders in the event of an operational disruption.



## 15A.9 Supervisory review and feedback

- 15A.9.1** **G** The *FCA* may provide individual *guidance* as to whether a *firm's* compliance with this chapter is adequate and, if necessary, require a *firm* to take the necessary actions or steps to address any failure to meet the requirements in this chapter.
- 15A.9.2** **G** A *firm* should have regard to the views provided by the *FCA* in relation to the *firm's* compliance. If a *firm* considers that any individual *guidance* given to it is inappropriate to its circumstances it should, consistent with *Principle 11* (Relations with regulators), inform the *FCA* that it disagrees with that *guidance*. The *FCA* may reissue the individual *guidance* if, after discussion with the *firm*, the *FCA* concludes that the appropriate actions or steps a *firm* should take is different from that initially suggested by the *FCA*.
- 15A.9.3** **G** If, after discussion, the *FCA* and a *firm* still do not agree, the *FCA* may consider other tools available to it, including its powers under sections 55J and 55L of the *Act* on its own initiative to require the *firm* to take specific steps in line with the *FCA's* view to comply with the requirements in this chapter.