



daisy.

# 6 STEPS TO BUILDING OPERATIONAL RESILIENCY

Produced by award-winning  
continuity and resilience  
consultant David Davies.

[daisyuk.tech](https://daisyuk.tech)



## David Davies, Business Continuity Consultant at Daisy, gives you his six most important steps to building operational resilience.

### 1. Define your important business services (IBS)

**As set out in the handbook of the Financial Conduct Authority (FCA) SYSC 15A. Important Business Services (IBS) are the key overarching services a firm delivers to its customers.**

What makes a business service “important?” The FCA Handbook explains it as a disruption to that service would cause “intolerable harm” to clients or be a risk to the UK financial markets.

What is a business service? A business service may span across the work of many departments and be dependent on many services such as IT services and supplier services. Payments or mortgages may be a business service, for example. The IT system that runs the mortgage service isn’t a business service, the finance department which handles the majority of mortgage payments isn’t a business service, these are dependencies that need to be mapped to the business service.

Applicable firms should have identified their **important business systems** by 31 March 2022\*.

### 2. Set your impact tolerances for each IBS

**The FCA Handbook defines impact tolerance as “maximum tolerable level of disruption” and is measured in time, and any other relevant measurements. To use the example, if the payments IBS failed for five minutes during a quiet period on a weekday afternoon there may be little impact. If it failed for longer it may cause “intolerable harm”.**

In this way, the firm can prioritise the urgency to recover services that are within the list of important business

systems. (as well as other services).

Applicable firms should have identified their **IBS impact tolerances** by 31 March 2022\*.

### 3. Map your dependencies sufficiently to have completed points 1 and 2

**Important business systems on their own are a bit abstract, it’s important to associate them with the departments, IT, suppliers and any other key dependencies which deliver them.**

This enables the firm to plan for the resilience of the IBS (potentially investing more to increase its resilience). It also enables the firm to focus recovery effort on the IBS during an incident, and to understand the dependencies which need to be tested to practice for an incident.

Applicable firms should have **mapped their IBS’ dependencies** by 31 March 2022\*.

### 4. Carry out scenario testing sufficiently to have completed points 1 and 2

**Scenario testing is important to validate the resilience and recovery capability of each IBS. This needs to be planned, and applicable for the dependencies.**

For example, IT services could be IT disaster recovery tested to prove that technology can failover, or recover from replicas or backups, while the key management decision-making for an IBS could be better tested by a simulation or paper-based exercise.

Applicable firms should have **scenario tested their IBS’ dependencies** by 31 March 2022\*.

### 5. Produce your first self-assessment document (to be updated regularly after that)

**Firms will also be expected to self-assess the status of steps 1-4 on a regular basis.**

The self-assessment itself is defined in the FCA handbook

SYSC 15A. As such, the FCA is making it clear that firms are expected to maintain the standards required of them.

Applicable firms should have a **self-assessment document** in place by 31 March 2022\*.

### 6. Operate and remain within impact tolerances

**The additional target is for firms to be able to demonstrate that they have mapped and tested important business systems to operate and remain within their impact tolerances.**

As such, if there are gaps in resilience and recovery capability these will need to be understood and closed.

Applicable firms should have this in place, “as soon as possible after 31 March 2022, and no later than 31 March 2025.”\*

**\*For more information on the FCA guidelines click here.**

#### About the author...

David Davies is an award-winning Business Resilience and IT Resilience Consultant at Daisy Corporate Services. He has worked in IT resilience and recovery for more than 20 years, starting in a technical role at IBM looking after data backups and testing disaster recovery on very large enterprise systems.

David moved on to project management of disaster recovery testing, then left IBM to work in business continuity consultancy over the last 15 years. In that time, David has worked with more than 150 organisations as a resilience consultant, some medium-sized but the vast majority being enterprise-sized organisations.





## **NEXT STEPS**

If you want to find out how Daisy can help you to improve your operational resilience, contact us on:

 **0344 863 3000**

**Or if you're an existing customer, get in touch with your account manager directly.**