Operational resilience: what IT can do

A plain-English guide to the part IT plays in keeping a regulated firm serving clients through disruption, including which FCA rules apply to you. This is general information, not legal or regulatory advice.

What operational resilience means

The Financial Conduct Authority's (FCA) operational resilience rules, in chapter SYSC 15A of its Handbook, ask firms in scope to identify their important business services, set limits on how much disruption they could tolerate, and test that they can stay within those limits. The transition period ended on 31 March 2025.

The rules apply to a defined list of firms, including enhanced scope SM&CR firms, banks, designated investment firms and Solvency II firms. Most small insurance brokers and advice firms do not appear to be on that list, but check your firm's status with your compliance adviser or the FCA.

Even if the rules do not apply to you, the questions below are a useful way to think about IT risk, and the new incident reporting rules further down have a much wider reach.

Where IT fits

For most firms, almost every important service depends on IT: the application that records client business, the email and phones used to deal with clients, and the connectivity that links them together. Mapping those dependencies is a practical first step.

Once you know what each service depends on, you can ask sensible questions. How long could we cope without this system? What would we do instead? How do we know recovery works?

Dependencies to map

- ✓ The main business application and its data
- ✓ Email, phones and video calls
- ✓ Internet connections and network equipment

- ✓ Cloud services and their suppliers
- ✓ The people who run each of these

Third-party providers

Many firms rely on outside suppliers for hosting, software, connectivity and IT support. The FCA's position is that a firm stays responsible for its important services even where a third party is involved, so it is worth understanding what your suppliers would do in a failure.

Useful questions for any supplier include where your data is held, how it is backed up, what happens if their service fails and whether recovery has been tested.

Testing and recovery

A plan that has not been tested is a hope. A practical test might be restoring a server from backup, switching a small group of users to a recovery environment or working through what happens if the office is unavailable for a day.

We have helped an insurance broker set up a recovery service on our private cloud that was later used for real. Having been through that, we can say that the plan, the people and the technology all matter, and that the first real use is a poor time to find a gap.

New FCA incident reporting rules from 18 March 2027

From 18 March 2027, all firms with a Part 4A permission must report operational incidents that meet the FCA's thresholds. That is much wider than the resilience rules, so it is expected to reach small brokers and advice firms.

A report is needed where a firm reasonably believes an incident poses a risk of intolerable harm to consumers that they cannot easily recover from, a risk to the safety and soundness of the firm or other market participants, or a risk to market stability, integrity or confidence. Planned outages and near misses do not have to be reported.

Most FCA-only firms make one short report through FCA Connect, as soon as practicable and within 24 hours of deciding that a threshold has been met. Larger firms have a fuller process.

A separate requirement to notify the FCA about material third-party arrangements and keep a register applies to a narrower list of firms, including enhanced scope SM&CR firms.

Agree with your IT provider

- ✓ How you will be told about an incident
- ✓ What they can tell you, and how quickly
- ✓ Who in the firm decides if it is reportable
- ✓ Who can submit a report if key people are away

Operational resilience: what IT can do: common questions

Do the resilience rules apply to my firm?

They apply to a defined list of firms, and most small brokers and advice firms do not appear to be on it. Your compliance adviser or the FCA can confirm your position.

Do the new incident reporting rules apply to small firms?

They apply to all firms with a Part 4A permission from 18 March 2027, but only incidents that meet the thresholds need reporting. Your compliance adviser can tell you how this applies to your firm.

Can you write our resilience plan?

Your firm owns its plan. We can describe the IT systems, how they are protected and how they would be recovered, so the plan is based on facts.

What should we do first?

List the services you could not do without, and the systems each one depends on. That is the starting point for everything else.

Talk to a technician: 03700 500 040 · enquiries@netvector.co.uk · itforfinance.co.uk
IT for Finance is operated by NetVector Consulting Limited, South Barn, Crockham Hill, Edenbridge, Kent TN8 6SR.
Registered in England and Wales No. 03401851.