Operational Resilience Self-Assessment

Ten questions a supervisor is likely to ask about your operational resilience framework, whether you are in scope of the PRA/FCA operational resilience rules, DORA, or both. It takes about ten minutes and shows where your framework is strong and where it is likely to be challenged.

How to score: tick one box per question. **Yes** = 2 points (in place, documented and evidenced), **Partly** = 1 point (exists but incomplete, out of date or not evidenced), **No** = 0 points. Answer for how things actually work today, not how the policy says they should.

	QUESTION	YES	PARTLY	NO
GOVERNANCE & SCOPE				
1	**Are your important business services identified and approved by the board, and reviewed in the last 12 months?** Including a clear rationale for what is in and out of scope.	☐	☐	☐
2	**Is your self-assessment document current, board-approved and something you could hand to a supervisor tomorrow?** Updated after material change, not only annually.	☐	☐	☐
MAPPING & TOLERANCES				
3	**Have you mapped the people, processes, technology, facilities, data and third parties behind each important business service?** Detailed enough to identify single points of failure.	☐	☐	☐
4	**Does every important business service have an impact tolerance, tested against severe but plausible scenarios?** With documented results and actions where a tolerance would be breached.	☐	☐	☐
ICT RISK & CONTROLS				
5	**Is there a documented ICT risk framework with a named owner, reviewed at least annually, with controls mapped to risks?** And evidence that the controls actually operate.	☐	☐	☐
6	**Can you classify and report a major ICT incident within your regulatory timelines?** Tested in an exercise, with clear decision-makers and pre-agreed templates.	☐	☐	☐
THIRD PARTIES				
7	**Is your third-party register (or DORA register of information) complete, including critical ICT providers and their key sub-contractors?** Including an assessment of concentration risk.	☐	☐	☐
8	**Do your critical third-party arrangements have exit plans that have been tested, not just written?** Covering both a planned exit and a sudden supplier failure.	☐	☐	☐
TESTING & SUSTAINABILITY				
9	**Do you run a resilience testing programme, with every finding tracked to closure and reported to senior management?** Scenario tests, disaster recovery tests and, where relevant, threat-led testing.	☐	☐	☐
10	**Could your own team absorb the next regulatory change or run the next RCSA cycle without external consultants?** The real test of whether the framework is owned or rented.	☐	☐	☐

Your score

Total (out of 20): _____

16–20 · Well placed
Your framework is likely to hold up to supervisory review. Focus on keeping evidence current and making sure the framework adapts as your business and the rules change.

9–15 · Gaps a supervisor would find
The framework exists but parts are incomplete, out of date or not evidenced. These gaps are usually fixable within weeks if prioritised now, before a review or incident exposes them.

0–8 · Material exposure
Significant elements are missing. Prioritise the board-level basics (questions 1, 2 and 4) and your critical third parties (questions 7 and 8) first.

Where most firms score lowest

Questions 4 and 8. Impact tolerances and exit plans are often written for the deadline but never tested. A supervisor will ask for test evidence, not the document.

Question 3. Mapping is frequently done once and not maintained, so it no longer reflects how services are actually delivered.

Question 10. Many firms built their framework with heavy consultancy support. If the knowledge left with the consultants, every regulatory change becomes a new project.

Scored below 16? Get an independent view.

Our **Operational Resilience Health Check** (£2,500, fixed price) tests your framework against DORA and PRA/FCA expectations and gives you a prioritised remediation roadmap. Or book a free 30-minute consultation to talk through your results.

sainul.hossain@resilientcontrol.co.uk · +44 7535 631101 · resilientcontrol.co.uk

This self-assessment is a general guide to help you reflect on your operational resilience framework. It is not legal or regulatory advice and does not replace a review of your firm's specific obligations. © 2026 Resilient Tech Risk and Control Ltd, trading as Resilient Control. Registered in England and Wales, Company No. 17500049.