



THE WORKING LIBRARY

Severe but Plausible: A Scenario Library

Twelve scenario outlines to seed an operational resilience testing programme. Each names the trigger, what to watch against your tolerances and one way to make the exercise properly severe.

How to use this library: pick scenarios that threaten your important business services specifically, then tune severity until the exercise genuinely risks breaching a tolerance. The supervisory criticism is rarely that firms did not test; it is that the tests could not fail. Assume the disruption occurs; the question a test answers is what happens next.

1 Designated cloud provider regional outage

A hyperscaler region hosting a critical workload degrades for a working day. Watch: which services breach tolerance before failover completes. Make it severe: the status page says investigating for the first four hours.

2 Ransomware in the core estate

Encryption detected across file services during the overnight batch. Watch: time to a trusted restore point and what data falls in the gap. Make it severe: the most recent backup shows signs of tampering.

3 Payment rail unavailable

A payment scheme your clients depend on rejects submissions from mid-morning. Watch: stuck value against the tolerance's further measures, not just elapsed time. Make it severe: the outage spans a peak settlement day.



4 Silent data corruption

A pricing or ledger feed has been writing bad records for three days before anyone notices. Watch: how far back remediation must reach and who tells affected clients what. Make it severe: the corruption spans a reporting boundary.

5 Critical supplier fails commercially

A material third party gives notice it will cease service in 30 days; insolvency practitioners are already in. Watch: whether exit plans work at reading speed, not signing speed. Make it severe: your second-choice supplier just took a large intake from other stranded customers.

6 Loss of the primary workplace

The main office is inaccessible from 07:00 with no re-entry estimate. Watch: which IBS actually depend on the building, versus which people assume they do. Make it severe: the outage includes the on-site comms room.

7 Concurrent key-person loss

Both people who genuinely understand a critical process are unavailable for a fortnight, at once. Watch: whether documented procedure lets someone competent-but-new operate the service inside tolerance. Make it severe: it happens during quarter end.

8 Cyber incident with confirmed exfiltration

An intrusion is confirmed and client data has left. Watch: the collision between forensic containment and service continuity, plus regulatory notification clocks. Make it severe: the affected system underpins your highest-priority IBS.

**9 Network provider failure**

The primary connectivity provider drops both supposedly diverse routes. Watch: whether diversity exists in fact or only in the contract. Make it severe: the fault also affects the branch or DR site.

10 Settlement or end-of-day failure

The end-of-day process aborts and the market deadline is three hours away. Watch: decision authority under time pressure and manual workaround capacity. Make it severe: the person who fixed it last time left in spring.

11 Software supply-chain compromise

A vendor pushes a poisoned update to software inside your estate. Watch: how quickly you can identify affected systems from your mapping. Make it severe: the vendor's advice conflicts with your regulator's expectations.

12 Extended power disruption

The data centre or a critical site loses power beyond generator autonomy. Watch: orderly-shutdown decisions and recovery sequencing against tolerances. Make it severe: it coincides with scenario 6.

Each exercise should end with the same three artefacts: a timed record of decisions, a verdict per tolerance (held, strained or breached) and a vulnerabilities list with owners. Those artefacts are what the self-assessment quotes and what supervisors ask to see.

Want the exercise designed and run for you?

The Scenario Testing Exercise takes a scenario from this library, tunes it to your services and tolerances, facilitates the tabletop and writes the evidence pack. Fixed fee, on the pricing page.

operationalresilienceuk.co.uk/pricing/

