

Operational Resilience

Operational resilience is how an organisation keeps its critical services running when something fails, and recovers them fast. Here is what it means, why regulators now require it and the one rule that holds it together.

WHAT IT IS

Operational resilience is the ability to keep your critical business services running through a disruption and recover them quickly when they fail. It assumes that outages, cyberattacks and supplier failures will happen, and focuses on protecting the service the customer relies on rather than preventing every incident. It is now a board-level duty, not an IT task.

WHY IT MATTERS

8.5 million

Windows devices crashed worldwide by one faulty software update on 19 July 2024.

Microsoft, 2024

500 million dollars

The cost to Delta Air Lines of that outage over five days, as reported to regulators.

Delta, SEC filing, 2024

200 of 290

Swedish municipalities disrupted when one shared supplier was hit by ransomware.

IMY, 2025

WHAT HAPPENED

In late August 2025 ransomware hit Miljödata, a Swedish supplier whose HR and work-environment systems are used by roughly 80 percent of the country's municipalities. Around 200 of Sweden's 290 municipalities were disrupted and about 2.2 million people's data was later exposed. The service failure was real for every municipality, even though the breach happened at a supplier. (IMY, 2025)

RED FLAGS TO WATCH FOR

Weak resilience shows up before the incident. Watch for these.

- You cannot quickly name your most important business services or who relies on them.
- No impact tolerance is set, so there is no agreed limit on how much disruption is too much.
- A recovery plan exists on paper but has never been tested from end to end.
- A critical service depends on a single supplier or provider.

THE ONE RULE THAT STOPS IT

Set an impact tolerance for every important business service, then test that the service can stay within it when something fails.

THEN BUILD THE HABIT AROUND IT

- Identify your important business services and who depends on each one.

- Map the people, systems, data and suppliers behind each service.
- Test against severe but plausible scenarios, including a key supplier going down.
- Give the board ownership of the approach and review it at least once a year.

MYTHS AND FACTS

MYTH

Operational resilience is just business continuity with a new name.

FACT

Continuity and recovery restore systems after they break. Resilience starts from the customer service and sets a limit on tolerable disruption, assuming failure will happen.

MYTH

Resilience is an IT problem.

FACT

It is a board duty. Under NIS2 Article 20 and the UK regime, senior management approves and owns the approach and can be held accountable.

MYTH

We are covered because our cloud provider is resilient.

FACT

Depending on one provider is a concentration risk. In July 2024 a single faulty update crashed about 8.5 million Windows machines.

THE LEGAL DUTY

Operational resilience is now a legal duty. DORA has applied across the EU financial sector since 17 January 2025, and NIS2 took effect in Sweden as Cybersäkerhetslagen on 15 January 2026, with boards accountable under Article 20.

GET HELP

eBuilder Security helps Swedish organisations identify their important business services, set impact tolerances and test recovery. Read the full guide at the link below.

[Read the Full Article →](#)