

When things go wrong, panic is expensive

Business continuity and disaster recovery that keeps your organisation operating through incidents, outages, and crises. Plans your teams can use under pressure, tested before reality does.

Incidents do not announce themselves politely

Systems fail, suppliers go offline, and cyber attacks arrive at the worst possible time. Most organisations have a continuity plan. Far fewer have one that anybody has read, let alone rehearsed.

We identify which processes are truly critical, what they depend on, and how long you can afford to be down. Then we build plans people can follow under pressure, and test them before reality does.

One plan. Every incident type.

Ransomware, supplier failure, insider threat, natural disaster, employee welfare. One structure your teams learn once and use for all of it.

What you are actually signing up for

Tailored, not off the shelf. We start from a framework proven across more than a decade of engagements, then build your plan around your actual processes, dependencies, and people. You are not filling in a template, and you are not paying us to reinvent one.

This is an engagement, not a product. Analysis, then plans, then testing. We do not hand over a document and leave you to interpret it.

Subscription or one-off. Subscribers receive ongoing updates, new playbooks as we write them, and refreshed strategies. Or take it as a single engagement.

Testing. Plans are validated through tabletop exercises with your team. See the separate Tabletop Exercises sheet.

It connects to incident response. Escalation paths and recovery steps are built to match how your incident response actually works, rather than sitting alongside it as a separate document.

What you end up with

- 01 **A documented business impact analysis.** Critical processes, what they depend on, and how long you can afford to be without them.
- 02 **Agreed RTO and RPO targets.** Signed off by the business, not assumed by IT.
- 03 **Continuity and recovery runbooks.** Role-based and step-by-step, written to be followed under pressure rather than filed and forgotten.
- 04 **A playbook library.** Ransomware, data compromise, DDoS, insider threat, lost and stolen devices, crisis communication, employee welfare, and post-incident analysis.

Who it is for

Critical-service operators.

Survive and recover when systems or suppliers fail.

Regulated industries.

Documented, tested continuity as evidence for auditors and regulators.

Complex environments.

Dependency mapping for organisations where recovery is harder than it looks.

From impact analysis to tested runbooks

01 Analyse. Business impact analysis to find critical processes and dependencies.	02 Define. Agree RTO and RPO targets with the business.	03 Plan. Design continuity and recovery runbooks integrated with incident response.	04 Test. Exercise the plans so teams know their roles before a real incident.	05 Review. Refresh on a regular cycle as systems and suppliers change.
--	--	--	--	---

Why Syndis

Based in Iceland, Sweden, and Poland. Serving clients globally.

We have been building continuity plans for Nordic organisations for over a decade, and every engagement sharpens the next. Subscribers get the benefit of that directly: new playbooks and refined strategies as we develop them, rather than a plan that starts ageing the day it is signed off.

ISO 27001

NIS2

DORA

GDPR

Be ready before the incident

Tell us what you need to keep running. We come back with scope and a timeline. We respond to most inquiries within one business day.

■ syndis@syndis.com

