

ASSESSMENT BROCHURE

Technical Resilience Assessment

Know exactly how well your critical systems can withstand, respond to and recover from serious disruption — and what to fix first.

A practitioner-led assessment. Not an audit. No pass/fail. No blame.

A STRUCTURED EVALUATION THAT GIVES YOUR TECHNICAL TEAMS

- 01** An evidence-based view of real recovery capability
- 02** A defensible maturity baseline
- 03** A prioritised, costed remediation roadmap they can act on immediately

For IT, cyber, infrastructure and application teams responsible for the resilience of critical systems.

THE CHALLENGE

Most organisations don't truly know how resilient their systems are

Every organisation assumes its critical systems will recover from a serious failure. Far fewer have tested that assumption against realistic, advanced or catastrophic scenarios.

Questionnaires and audits produce scores and checkboxes but they rarely reveal whether your teams can actually detect, respond to and recover from a real disruption when it happens.

The gap between **assumed resilience** and **demonstrated resilience** is where the real risk sits.

When a platform fails, data is exfiltrated, or a key dependency collapses, that gap becomes very expensive very quickly.



The Technical Resilience Assessment gives you an honest, evidence-based answer — and a clear plan to close the gap.

WHAT IT IS

An assessment, not an audit

A Technical Resilience Assessment (TRA) is a structured, practitioner-led evaluation of how well a defined technology domain – a platform, application environment or critical system – can withstand, respond to and recover from serious disruption.

There are no pass/fail grades, no blame and no box-ticking. Instead, your technical teams work through realistic, advanced and catastrophic failure scenarios alongside our facilitators, describing exactly how they would detect, respond and recover.

Capability is then scored against the **CM-Alliance Resilience Maturity Model** – a proprietary five-level framework ranging from Level 0 (Unprepared) to Level 4 (Operationally Resilient).

The CM-Alliance Resilience Maturity Model A five-level framework to assess and strengthen your organisational resilience.			
LEVEL	LABEL	WHAT IT MEANS	RISK LEVEL
0	 Unprepared	 No documented procedures, no backups, no testing. Critical risk.	 CRITICAL RISK
1	 Ad Hoc	 Informal or undocumented; relies on individual knowledge. High risk.	 HIGH RISK
2	 Documented	 Procedures documented; backups configured; not regularly tested. Moderate risk.	 MODERATE RISK
3	 Validated	 Documented and tested within the last 12 months; redundancy validated. Low risk.	 LOW RISK
4	 Operationally Resilient	 Automated detection and response; continuous testing; quarterly drills. Minimal risk.	 MINIMAL RISK

THE CM-ALLIANCE RESILIENCE MATURITY MODEL

The result: an honest picture of your current resilience, a defensible maturity baseline, and a remediation roadmap your teams can act on straight away.

HOW IT WORKS

Minimal demand on your team. Maximum insight.

1

Scoping conversation

A short call to define the domain to assess — for example, an application hosting platform or a payments environment — and to define and agree who should take part.

2

A single focused session

One to two hours, facilitated by experienced resilience and cyber practitioners. We do the rest.

3

Scenario-based evaluation

Your teams work through realistic disruption scenarios — typically catastrophic platform failure or unavailability, application-layer data exfiltration or compromise, and infrastructure dependency failure. Each tests detection, response and recovery.

4

Maturity scoring

Capability is scored per scenario against the CM-Alliance Resilience Maturity Model.

5

Your report, delivered

Detailed technical findings, evidence observed, documented areas of strength, and a consolidated table of prioritised recommendations with timelines, effort and ownership.

1–2 hrs

The assessment itself is a single facilitated session — minimal disruption to your team's day-to-day operations.

WHAT MAKES IT DIFFERENT

Practical, evidence-based and built for technical teams

Practitioner-led

Facilitated by experienced resilience and cyber practitioners, not questionnaire administrators.

Scenario-based

Built around realistic disruption scenarios rather than abstract questionnaires.

Evidence-informed

Findings are based on facilitated discussion and supporting evidence where available.

Maturity-scored

Capability is assessed against a defined, proprietary resilience maturity model.

Remediation-focused

Recommendations are practical, prioritised and aligned to technical ownership.

Collaborative, not punitive

The purpose is to find improvement opportunities, not to blame individuals.

Minimally disruptive

The assessment itself is a single 1–2 hour session.

WHAT YOU RECEIVE

A confidential, actionable report

Each Technical Resilience Assessment delivers:

- | **Detailed technical findings**, with evidence observed
- | **A maturity score per scenario**, mapped to the CM-Alliance Resilience Maturity Model
- | **Documented areas of strength**
- | **A consolidated set of prioritised recommendations** — each with rationale, timeline, effort and cost, required resources, implementation steps and success criteria
- | **A consolidated remediation roadmap** mapping every action to a clear owner and priority

A BOARD-READY COMPANION OPTION

The Operational Resilience Assessment (ORA) translates these same findings into business impact, growth implications and regulatory relevance for board and risk-committee audiences.

Take either on its own — or both, with one the natural next step from the other.

NEXT STEP

Is your resilience?

You can't fix what you can't see. The Technical Resilience Assessment replaces assumption with evidence. It shows you exactly how prepared your critical systems really are, and precisely what to fix first.

It starts with a short scoping conversation: we'll define the domain to assess, agree on the scenarios, and confirm who should be in the room.

One session. One clear roadmap.

[Book a scoping call](#)

[Request the full assessment outline](#)

[Speak to our resilience team](#)