RESILISCORE

Cyber Resilience Maturity Assessment Report

Company
TESTING123

Assessment date
7 March 2026

Report reference
RS-1CA45FA6

Overall score
2.42 / 5

D - Repeatable

Key Findings

Current resilience posture

Your organisation shows a Repeatable maturity level (2.42 / 5). Relative strengths are currently more visible in Asset, Threat, Suppliers. Priority improvement areas are Governance, Risk, Identity.

Highest priority improvements

Governance & Leadership (2.10 / 5)
Risk & Compliance (2.20 / 5)
Identity & Access Management (2.30 / 5)

Immediate actions

Introduce a 1-page leadership dashboard (KPIs + priorities).
Set treatment timelines for high risks.
Run access reviews for sensitive systems.

Executive Summary

Overall result

Overall score: 2.42 / 5 Grade: D Maturity: Repeatable

0 5

Risk signal

Moderate risk

Interpretation (consultant view)

Defined practices exist. Next step is consistency, measurement and proof they work under pressure.

Lift the weakest domains to remove single points of failure.

Introduce lightweight assurance: testing, evidence, and simple KPIs.

Top priorities (weakest domains)

Governance & Leadership	2.10
Risk & Compliance	2.20
Identity & Access Management	2.30

Key strengths (highest domains)

Asset & Data Management	3.00
Threat & Vulnerability Management	2.90
Third-Party & Supply Chain	2.80

Maturity score and grade explained

This page explains what your maturity score and grade mean in plain language. Resilscore uses a 0-5 maturity scale to measure whether key resilience controls exist, operate consistently, and can be evidenced.

Your overall result

Overall score: 2.42 / 5 Grade: D Maturity label: Repeatable

0 5

Risk signal

Moderate risk

Grade bands (A to E)

- A: 4.50 - 5.00 Optimised (measured, tested, improving)
- B: 3.50 - 4.49 Managed (consistent, owned, repeatable)
- C: 2.50 - 3.49 Defined (documented, uneven consistency)
- D: 1.50 - 2.49 Repeatable (some routine, notable gaps)
- E: 0.00 - 1.49 Not in place (informal, reactive)

How to interpret your score (SME guidance)

- Your score is a snapshot of maturity today, based on your responses. It is designed to help prioritise improvements that reduce disruption risk (cyber).
- Moving up is usually less about buying tools and more about three things: ownership (someone is accountable), cadence (it happens regularly), and evidence (you can prove it quickly).
- Focus on lifting the lowest 2-3 domains first. That typically removes the biggest single points of failure and improves overall resilience fastest.

How the score is calculated (simple)

- Each question is scored from 1 to 5.
- Each domain score is the average of the questions in that domain.
- Overall score is the average of the domain scores.
- Grade is derived from the overall score using the bands above.

Framework mapping (plain English)

Resiliscore includes framework mapping to help SMEs translate improvements into language that customers, auditors, insurers, and procurement teams recognise. This is not a certification. It is guidance to support alignment and reporting.

Why these frameworks were selected

- NIST CSF is widely understood as a practical structure for cyber outcomes (identify, protect, detect, respond, recover).
- ISO 27001 / 27002 themes are common reference points for policies and controls, especially for supplier assurance and audits.
- Using familiar language reduces the friction of questionnaires and improves the quality of due diligence conversations.

How mapping is implemented in Resiliscore (in practice)

- Each question is tagged to one or more framework themes (for example: access control, backups, incident response, supplier assurance).
- When you improve a control in the 30/60/90 plan, you are also improving the related framework themes that buyers and auditors ask about.
- Mapping is used to support reporting and evidence, not to replace formal compliance work or audits.

How this affects SMEs (the benefit)

- Faster questionnaires: reuse a consistent evidence set instead of answering from scratch each time.
- Clearer priorities: improvements tie back to recognised themes, making investment easier to justify.
- Better credibility: you can explain controls in a way that procurement teams recognise without needing heavy compliance overhead.
- Reduced panic: evidence and ownership mean you can respond quickly to customer security questions.

Important note

Framework mapping is guidance. Resiliscore is designed as an SME resilience tool and does not provide certification. If you need formal compliance or audit outputs, use these mappings as a starting point for structured work with an expert.

Results Visuals

Ranked domains (weakest first)

Governance	2.10
Risk	2.20
Identity	2.30
Response	2.30
Operations	2.40
Recovery	2.50
Suppliers	2.50
Threat	2.50
Asset	3.00

How to read this

The radar shows relative maturity by domain (0-5 scaled). Bigger shape = more consistent controls.

The ranked list highlights where disruption risk is most likely to come from first.

Focus on lifting the lowest 2-3 domains - that usually produces the fastest overall improvement.

Domain Risk Priority (RAG View)

This view highlights which resilience domains require the most immediate attention. Domains are grouped using a Red-Amber-Green (RAG) model based on maturity scores.

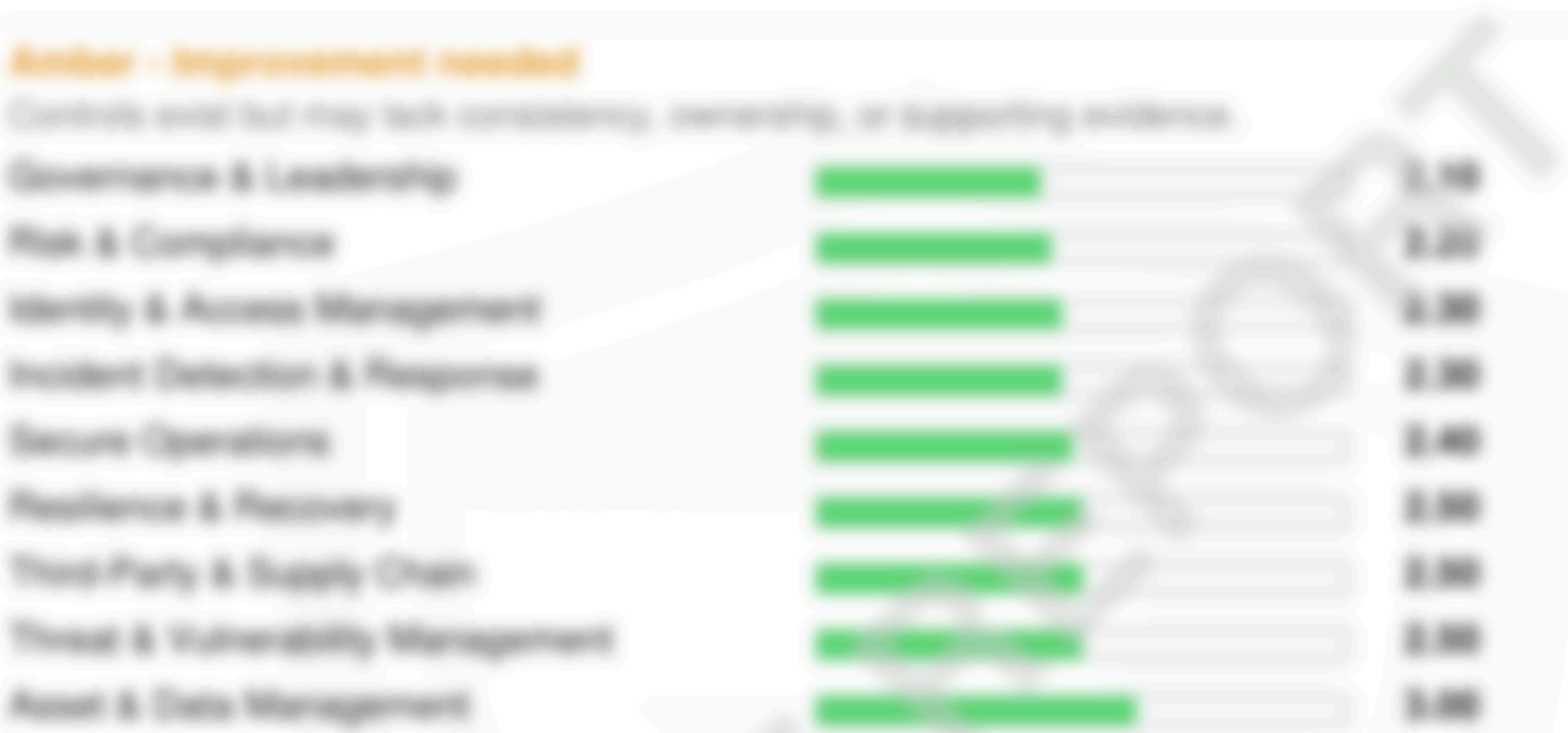
Red – Priority attention

These domains represent the greatest resilience exposure and should typically be prioritised for improvement.

None at present.

Amber – Improvement needed

Controls exist but may lack consistency, ownership, or supporting evidence.



Green – Relative strength

These domains demonstrate stronger operating practices relative to the rest of the organisation.

None at present.

Priority guidance: focus improvement efforts first on Red domains, then stabilise Amber domains, while maintaining Green domains through routine monitoring.