



SAFE

Cyber resilience assessment and improvement framework

Evolve from one-off technical reviews and isolated security fixes, to a dynamic resilience model that delivers ROI with every cycle.



Contents

SAFE, explained

A clear process that continually assesses and improves resilience

Why SAFE matters

Cyber resilience is now a leadership issue

Why business leaders invest in SAFE

The value of greater resilience clarity

SAFE is more than a health check

Resilience needs a cycle, not a snapshot

The SAFE cycle

Assess. Prioritise. Improve. Repeat.

What you get from each SAFE stage

Outputs, reports, visual improvement data and more for GRC and to share with the board

The value of ongoing SAFE cycles

Strengthening your resilience over time

What clients value about SAFE

Build a clear cyber resilience strategy

SAFE, explained

A clear process that continually assesses and improves resilience

SAFE helps organisations **measure cyber maturity, identify business-critical gaps, and invest for maximum returns.**

Our cyber resilience framework assesses your organisation's security posture. You understand, see and can report where the real risk sits, driving what should happen next. Resilience-focused organisations need more than a one-off technical review. SAFE delivers evidence-based resilience cycles that support better decisions, stronger governance, and more effective security investment.

Key points

SAFE gives senior leaders a quarterly business-aligned view of security risk, maturity, and priorities. It creates an ongoing cycle of assessment, provable progress, prioritisation, and improvement that strengthens resilience over time.

A SAFE business has ...

- Clear view of current cyber resilience and security posture
- Prioritised investment roadmap based on business risk and impact
- Regular reports to show progress and support GRC
- Stronger board and insurer confidence
- Significantly improved resilience posture over time



Book a SAFE discussion

Why SAFE matters

Cyber resilience is now a leadership issue

Resilience businesses understand that security is no longer just a technical concern.

It spans operational continuity, leadership confidence, regulatory readiness, insurer scrutiny, supplier trust, and the organisation's ability to grow safely.

Many organisations have controls in place, but fewer have a clear, evidence-based view of how resilient they really are. SAFE helps leaders move from fragmented security activity and unclear priorities to a more structured, measurable, and defensible cyber resilience strategy.

Leaders use SAFE because they need:

- Stronger resilience planning
- Clearer board-level oversight
- Better prioritisation of security investment
- Improved confidence in budgeting decisions
- More credible insurer and audit conversations
- Clearer evidence of progress over time



Why business leaders invest in SAFE

SAFE helps senior leaders answer the questions that matter before risk tips into disruption, unplanned spend, or loss of confidence.

It underpins cyber investment with considered, defensible business decisions.

- **How do I know where resilience is weakest?**
Scores across 19 key GRC domains with 30+ page reports and visual data clearly reveal weakest areas.
- **How do I prioritise investment with more confidence?**
Colour-coded scoring grades areas for investment based on potential business impact and achieving fast improvement.
- **How do I strengthen board and insurer conversations?**
Presentable evidence and measured progress counter scrutiny concerns, support planning and prove insurability.
- **How do I reduce reactive decision-making?**
Replace fragmented security activity with a clear roadmap and better sequencing aligned to your business objectives.
- **How do I show improvement over time?**
SAFE delivers detailed analysis and visual proof, ready to share with key stakeholders and third parties.

SAFE: more than a health check

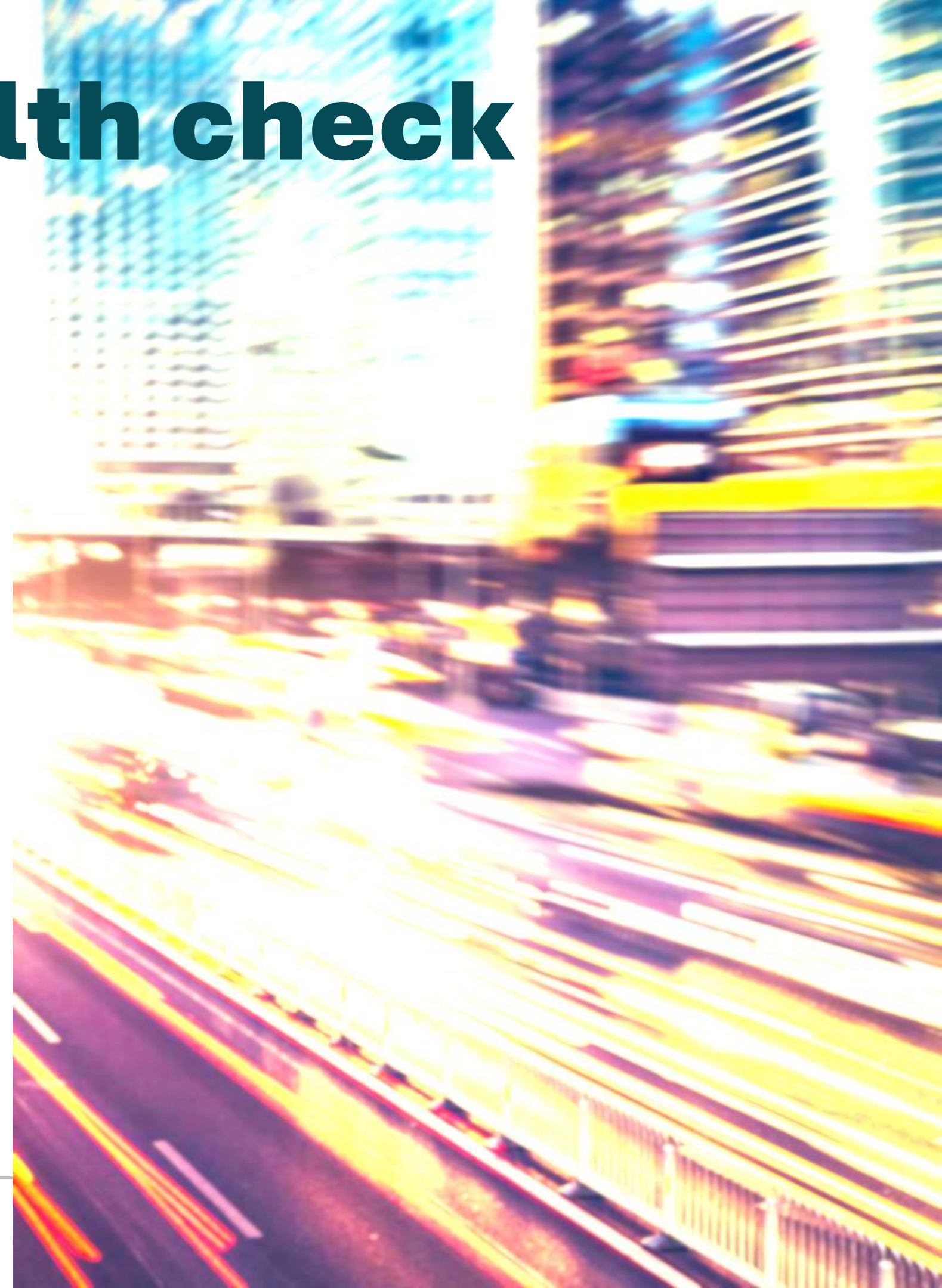
SAFE is ongoing because a one-off assessment can only highlight issues. Cyclical assessment is needed to create resilience in our fast-moving world.

Cyber threats never stay still. Attack surfaces expand. Business priorities shift. Technology estates evolve. *Without regular reassessment, yesterday's confidence can quickly become today's blind spot.*

SAFE delivers dynamic assessment that helps organisations stay agile, adaptive, and aligned to changing risk. It is:

- Not a one-time report
- Not a box-ticking exercise
- Not just compliance support
- A repeatable resilience framework
- A structured basis for continuous improvement

SAFE helps turn cyber security from a reactive concern into ongoing, improving, resilience capability.



The SAFE cycle

SAFE follows a simple, practical cycle that makes cyber resilience easier to understand, communicate, and improve.

1. Assess

Build a clear, evidence-based view of your cyber resilience, security posture, and maturity across 19 key domains.

2. Prioritise

Turn findings into visual data that determine clear priorities, so leadership attention, budget, and action are focused where they matter most.

3. Improve

Create a practical roadmap for resilience improvement, then reassess regularly as threats evolve and the attack surface changes.



What you get from each SAFE stage



1. Assess

You get:

- Baseline of current cyber maturity
- Strengths, weaknesses, and blind spots
- Understanding of where risk is highest



2. Prioritise

You get:

- Scored findings and visual summaries
- Clarity of what matters most and why
- Basis for investment & board discussion



3. Improve

You get:

- Prioritised roadmap to reduce risk
- Practical next steps and sequencing
- Ongoing review and measurable progress

What you receive from a SAFE assessment

Visual data

SAFE produces practical outputs that support leadership, planning, and action.

You receive:

- Evidence-based cyber resilience assessment
- A clear view of current security posture
- Maturity scoring across 19 key GRC domains
- Visual summaries for leadership discussion
- Prioritised and practical security roadmap
- Stronger input into budgeting and sequencing
- Baseline for future reassessment and benchmarking

The value lies not just in the thorough reports.
It is the clarity and direction they create, and their multiple uses for your team.

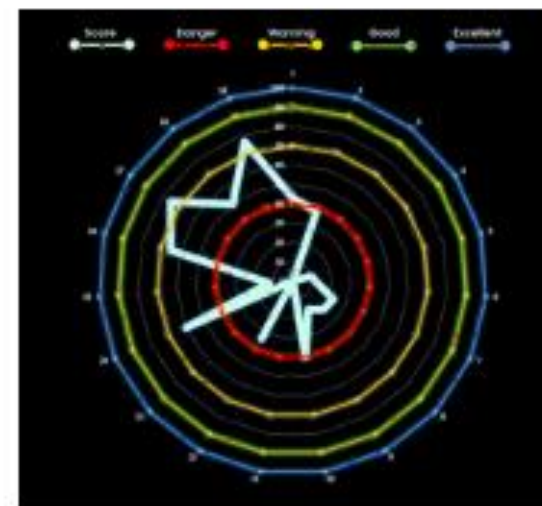


Sub-Area	Performed - 30%	Managed - 25%	Documented - 20%	Reviewed - 15%	Optimised - 10%
Formal review at executive level (10)	10				
Formal discussions at executive level (10)	10				
Executive oversight and ownership (10)	10				
Measured according to industry standards (25)		25			
Agree and formalise the standards of measure (10)			10		
Agree on and document the process (5)			5		
Document program ownership & responsibilities (5)			5		
Clear review process defined (5)				5	
Review process performed consistently (5)				5	
Review carried out at least once per year (5)				5	
Optimisations captured from review process (5)					0
Optimisations applied in line with process (5)					0
	30	25	20	15	0

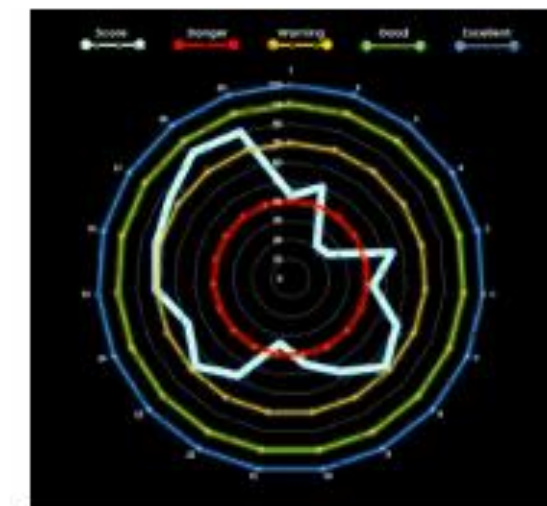
Baseline SAFE Score



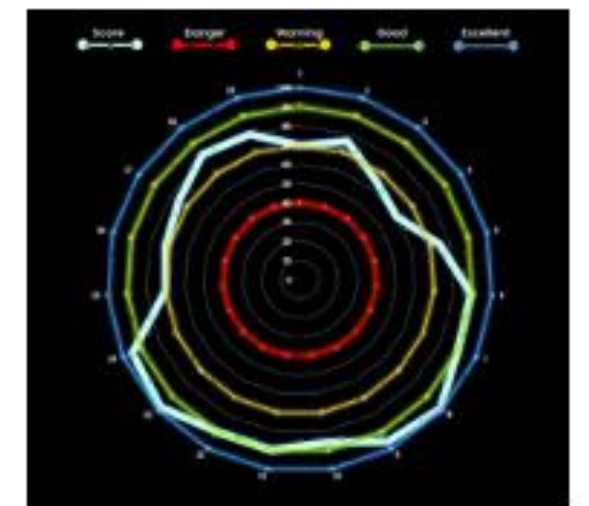
Day Zero



6-month retest



12-month retest



The value of ongoing SAFE cycles

The real value of SAFE comes from using it as an ongoing strategic framework, not a one-time exercise.

A one-time security snapshot is quickly out of date.

Ongoing reviews are the only way for leadership teams to clearly track and prove resilience maturity, justify investment, and demonstrate improvement over time.

- Cyber maturity builds, keeping you resilient as threats quickly evolve
- Clear evidence drives informed decisions and supports ongoing GRC
- Cyber resilience strategy and business priorities remain aligned
- Investment planning is rooted in truth and more disciplined
- Emerging exposures are identified fast
- Leadership and board work harmoniously to aligned targets, with agreed ROI

Regular SAFE assessments help organisations stay resilient as threats evolve and the attack surface expands, with clear evidence of ROI at every step.



What clients value about SAFE

“SAFE from ITHQ is not an audit, it's an evidence-based discussion with proportional outcomes aligned to business needs. When management sees the old reports compared with the new ones, they can see exactly where [my budget's] gone, where the time and effort's gone ... We can basically prove: 'Look at the difference we've made.' The SAFE reports provide an independent view of our systems like Pen Tests and are 32 pages long: very useful in many regulation-centric scenarios.

Mark Petar, Head of Systems, Montanaro

We couldn't do it without ITHQ

Philip Mitchell, Chief Infrastructure Officer, The Hippodrome Casino

SAFE gives leadership teams a clearer, more credible way to show resilience progress over time.





ITHQ | SAFE

Build a clear cyber resilience strategy

Regular SAFE cycles help turn cyber security into clear, measurable, adaptable, business-aligned resilience.

Talk to us

transform@ithq.pro

020 3997 7979



Book a SAFE discussion