secarma®
CYBERSECURITY EXPERTS

A Advise   C Certify   T Test

Cybersecurity Scorecard

Start understanding cyber risk without over-engineering the process.

This consultant-reviewed assessment gives organisations a clear, honest view of their current cyber resilience. It supports prioritisation and confidence, without the time, cost, or commitment of a full consultancy engagement.

What is the Scorecard?

This structured self-assessment evaluates how effectively your organisation manages cyber risk across key security domains.

Responses are combined with expert review and a scoring system. This delivers a clear baseline of your current security posture and highlights practical, prioritised next steps for improvement.

It is ideal for organisations that want insight and direction before committing to deeper assessments, testing, or certification. The Scorecard helps organisations understand where they stand today and where to focus next.

Business Benefits

Clarity without complexity - Gain a clear view of your cyber resilience without the overhead of a full assessment.

Prioritised action - Understand what to improve first and where to invest for the greatest impact.

Consultant-verified insight - Your results are reviewed by a Secarma consultant, ensuring findings reflect real-world risk, not just theory.

Reduced uncertainty - Make informed decisions with confidence before moving into testing, certification, or tooling.

A foundation for growth - Establish a baseline that supports future security improvement as your organisation evolves.

What the Scorecard Covers

The Cybersecurity Scorecard assesses your organisation across four core security areas:

Secure Configuration - How systems and services are configured to reduce exposure, including access control, patching, and baseline security controls.

Monitoring and Detection - How effectively threats and incidents can be identified through logging, monitoring, and alerting capabilities.

Incident Response - How prepared your organisation is to respond to and recover from incidents, including escalation, containment, and recovery planning.

Risk Management - How cyber risks are identified, owned, and managed across the organisation, including governance, policies, and accountability.

What You Receive

Your report evaluates how security is managed in business practices including

- Governance
- Technical Controls
- Operational Processes
- Incident Readiness.

The Scorecard Model

Each area is explored through focused questions that assess both the existence of controls and how effectively they are applied in day-to-day operations.

Responses are measured against a defined maturity model, creating a consistent baseline that reflects practical risk rather than documentation alone. All submissions are reviewed by a Secarma consultant to validate context, remove ambiguity, and ensure scoring reflects how security operates in practice.

Digital Delivery, Scoring, and Outputs

The Scorecard is completed and delivered entirely through the Secarma client portal.

Clients complete a guided online assessment at their own pace, with progress saved automatically. Once submitted, consultant review, scoring, and reporting are handled digitally within the same platform.

The resulting report provides an overall cyber resilience score, maturity ratings across each security area, and a clear view of strengths and gaps. Recommendations are prioritised based on risk and impact, enabling teams to understand what to address first and where effort will deliver the greatest improvement.

Who Is It For?

The Cybersecurity Scorecard is well suited to organisations that:

- Know cybersecurity matters but aren't sure where to start
- Want clarity before committing to testing or certification
- Need evidence to support internal decision-making or budgets
- Are preparing for Cyber Essentials, ISO 27001, or further assurance
- Want a low-risk, high-value starting point for improvement

Pricing

Cybersecurity Scorecard from **£500**

- Fixed scope
- Consultant reviewed
- No long-term commitment required

The Scorecard is often used as a credited stepping stone into follow-on services.

What Happens Next?

The Cybersecurity Scorecard is designed to support action, not just insight.

Results can be used to guide security planning, support internal discussions, and prepare for further testing or certification. Because results are retained within the portal, organisations can reassess over time and track improvement as controls mature, creating a clear and proportionate path into wider security services.

Based on your results, organisations typically move into one or more of the following areas:

Advise

Security roadmaps, policy development, vCISO support, third party assessments, incident response exercising and targeted consultancy.

Certify

Preparation and support for Cyber Essentials or ISO 27001.

Test

Penetration testing, vulnerability assessments, configuration reviews and assurance testing.

The Scorecard ensures your next step is informed, proportionate, and aligned to your risk profile.

Getting Started

If you're looking for clarity, confidence, and direction without over-engineering your approach to security, the Cybersecurity Scorecard is the ideal place to start.