Quorum Cyber

Service Description Security Maturity Assessment G Cloud 15

+44 333 444 0041
quorumcyber.com
Verdant, 2 Redheughs Rigg, Edinburgh, United Kingdom, EH12 9DQ

Table of Contents

Service Overview

Background

A Quorum Cyber Security Maturity Assessment (SMA) provides organisations and security leaders with a clear, objective understanding of how mature, consistent, and embedded their information security capabilities are across people, process, and technology. Many organisations operate security controls that have evolved organically over time, resulting in inconsistent implementation, unclear ownership, and limited visibility at an executive level. The SMA addresses these challenges by establishing a structured, repeatable baseline of security maturity, enabling leadership to prioritise improvement initiatives, align investment to risk, and strengthen governance.

It helps organisations translate complex technical risk into business-relevant insights that executives and boards can understand, while improving preparedness for incidents through stronger detection, response, and recovery capabilities. By aligning security activities to risk-based priorities and providing a common structure to manage regulatory obligations, a security maturity assessment enables more effective investment decisions, clearer accountability, and a more resilient, organisation-wide security culture.

Quorum Cyber's Solution

Quorum Cyber's Security Maturity Assessment (SMA) service evaluates the design, implementation, and effectiveness of information security controls across the organisation against industry best practice and recognised frameworks, such as NIST Cybersecurity Framework (CSF), ISO/IEC 27001, and CIS Critical Security Controls, the assessment applies a maturity-driven approach to determine not only whether controls exist, but how consistently they are applied, governed, and operating in practice.

The assessment identifies strengths, weaknesses, and gaps across governance, protection, detection, response, and recovery, helping organisations understand how prepared they are to defend against threats and manage incidents. It includes a detailed evaluation of security controls and can be tailored to specific organisational requirements and chosen standards, providing a clear, structured view of security maturity and readiness.

The insights from the assessment enable organisations to strengthen overall resilience by prioritising risk mitigation, improving regulatory and assurance alignment, and optimising the use of resources. The service delivers practical, actionable recommendations and a prioritised roadmap to enhance security strategy, improve operational effectiveness, and support long-term cyber resilience. Grounded in proven methodologies and frameworks such as NIST CSF, Quorum Cyber's approach helps organisations make informed, business-aligned decisions to strengthen defences and achieve measurable security improvement.

Differentiators

By partnering with Quorum Cyber on a Security Maturity Assessment, organisations gain access to our Centre of Excellence and deep cybersecurity expertise. Our team leverages globally recognised security benchmarking frameworks, including the NIST Cybersecurity Framework (CSF), to deliver a rigorous, detailed assessment that provides confidence in the findings and supports the development of targeted recommendations and practical roadmaps.

The Quorum Cyber Security Maturity Assessment (SMA) provides a structured, evidence-based evaluation of your organisation's information security capabilities, measuring the effectiveness and consistency of security controls across people, process, and technology.

The assessment is underpinned by recognised industry frameworks (e.g., NIST CSF, ISO/IEC 27001, CIS Controls) and applies a maturity-driven lens to determine not just whether controls exist, but how well they are embedded, governed, and operating in practice.

Service Features

- Framework-aligned maturity assessment across people, process, and technology
- Evidence-based review of policies, procedures, and technical controls
- Workshops with control and process owners
- Objective maturity scoring and benchmarking
- Actionable, prioritised improvement roadmap

The resulting assessment report includes:

- Executive-Level Maturity Dashboard – A clear visual representation of current and target maturity levels, enabling leadership to quickly understand strengths, gaps, and areas of concern.
- Framework-Mapped Maturity Scoring – Objective maturity ratings aligned to industry standards, supporting benchmarking and year-on-year improvement tracking.
- Control Effectiveness Insights – Identification of control weaknesses, inconsistencies, and dependencies that impact overall security performance.
- Actionable Improvement Roadmap – A prioritised, phased roadmap to progress security maturity in line with organisational risk appetite and strategic objectives.
- Foundation for Continuous Improvement – Establishes a baseline maturity position to support future assessments, regulatory readiness, and long-term security programme development.
- This approach goes beyond simply identifying gaps, focusing instead on delivering best-practice recommendations tailored to your organisation's specific risk profile and objectives. The value of the engagement lies in clear, actionable outcomes providing transparency into what is working well, where improvements are required, and a structured path to achieving enhanced cyber resilience.

Service Benefits

- Clear Visibility of Cyber Risk

  Provides an objective view of your current security posture, highlighting strengths, weaknesses, and critical gaps across people, process, and technology.

- Improved Risk Prioritisation

  Translates technical findings into risk-based insights, helping organisations focus investment and effort on the areas that will have the greatest impact.

- Stronger Incident Readiness and Resilience

  Identifies gaps in detection, response, and recovery capabilities, improving preparedness for cyber incidents and reducing business disruption.

- Alignment of Security Strategy to Business Goals

  Supports informed decision-making by aligning cybersecurity initiatives with business objectives, regulatory expectations, and organisational risk appetite.

- Benchmarking Against Best Practice

  Measures your maturity against recognised frameworks such as NIST CSF, enabling defensible comparisons and improved assurance for leadership, customers, and regulators.

- Foundation for Future Assessments

  Establishes a strong baseline to support cyber resilience assessments, regulatory reviews, and certification programmes.