Quorum Cyber

Service Description Certification Readiness G Cloud 15

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

Table of Contents

Service Overview 3

Background 3

Quorum Cyber's Solution 3

Differentiators 4

Service Features 5

Service Benefits 6

Service Overview

Background

Cyber security certification, such as Cyber Essentials+ or alignment with standards like ISO 27001 and SOC2 , provides independent assurance that an organisation manages cyber risk in a structured, consistent, and credible manner. In an environment of increasing cyber threats, regulatory expectations, and customer scrutiny, certification demonstrates that cyber security is being addressed as a core business risk rather than an ad hoc technical concern.

From a governance and compliance perspective, certification provides clear evidence of due diligence and supports alignment with legal, regulatory, and contractual requirements. Many customers, partners, and regulators now mandate certification as a condition of doing business. Achieving and maintaining certification therefore reduces commercial barriers, strengthens supply-chain trust, and supports competitive advantage.

Certification also drives consistency and continual improvement. Independent assessment helps identify gaps that may not be visible internally and provides a structured framework for improving people, process, and technology controls over time. This reduces the likelihood and impact of cyber incidents while improving organisational resilience and incident readiness.

Quorum Cyber provides a structured, consultative approach to certification readiness, designed to support organisations seeking clear guidance and direction throughout the preparation process. The service establishes a baseline of existing security controls and practices, identifies gaps against relevant certification requirements, and assesses the quality, consistency, and availability of supporting evidence. This enables organisations to gain a clear and accurate understanding of their current readiness and areas requiring improvement.

Based on these findings, Quorum Cyber delivers a practical, prioritised remediation roadmap to guide organisations toward successful certification. The service supports preparation for ISO 27001, Cyber Essentials Plus, and SOC 2, helping organisations reduce audit risk, improve security maturity, and demonstrate credible assurance to customers, regulators, and stakeholders.

Quorum Cyber's Solution

This service assesses an organisation's existing security controls, policies, and operational practices to establish how effectively information and systems are protected today. Through a structured review, gaps are identified against recognised security standards, enabling organisations to understand their current level of maturity and readiness. The assessment provides clear, prioritised insight to support remediation planning and reduce the risk of issues during formal audits or certification processes.

The service supports preparation for:

- ISO 27001, the international standard for establishing, implementing, and continually improving an Information Security Management System
- SOC 2, which evaluates how organisations manage and protect customer data in line with the Trust Services Criteria
- Cyber Essentials+, the UK government-backed scheme focused on protecting organisations against common cyber threats.

By aligning controls and practices to these standards, organisations can strengthen their security posture, demonstrate due diligence to customers and regulators, and achieve certification with greater confidence and efficiency.

Differentiators

The sole purpose of Quorum Cyber is to provide cost-effective cyber resilience through outcome-based Security services that are operationally excellent, technically advanced, and economically viable.

We are committed to providing exceptional security by utilising the latest technologies and methodologies to safeguard your assets and data. Our distinctive approach to security sets us apart within the industry.

By focusing on results, we customise our services to meet your specific requirements and objectives, ensuring that you have confidence in the management of your security.

Founded in 2016, today we are a team of 350+ experts. Our style is defined by three key characteristics:

People First: We lead with empathy, creating healthy conversations and driving positive change. We focus on the people first, the processes after, and only then on technology as a force multiplier to do more with less.

Technical Professionalism: We take pride in being a safe pair of hands that bring skills and experience to all situations.

Deep Partnership: We focus on understanding your specific requirements and circumstances, your own individual threat posture, risk landscape, risk appetite, and business strategy. Only by achieving true customer intimacy can we do our best work.

Service Features

Our certification readiness service supports ISO 27001, SOC 2, and Cyber Essentials Plus. Depending on the certification within scope, the following steps outline the indicative approach taken to deliver this service:

- Scoping and Boundary Definition
- Control Mapping and Gap Analysis
- Governance and Risk Management Review
- Policy and Documentation Assessment
- Technical Control Validation
- Operational Effectiveness Testing
- Third-Party and Supply Chain Assessment
- Remediation Planning and Audit Readiness

Service Benefits

This structured approach reduces audit risk, improves confidence, and supports successful certification or assurance outcomes.

- Reduced Operational and Service Delivery Risk

  Supports the identification and management of cyber risks that could disrupt essential services, compromise sensitive information, or impact public trust.

- Increased Assurance and Public Confidence

  Provides independent validation that appropriate security controls are in place, strengthening confidence among stakeholders, partners, and the public.

- Stronger Governance and Accountability

  Establishes clear ownership, oversight, and accountability for cyber security, aligning with public sector governance and risk management principles.

- Procurement Readiness and Supplier Assurance

  Enables organisations to meet mandatory or expected security requirements within government procurement and supply chains, reducing risk across public sector ecosystems.