



Service Description

Cyber Resiliency Assessment

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

Quorum Cyber extends its professional services and advisory portfolio with GRC Advisory Services, designed to support organisations at all stages of their cyber resilience journey. Many organisations face challenges in establishing direction, managing legacy technologies, or operating with processes that have not been shaped by a strategic, risk-based approach.

To help organisations evaluate the effectiveness of their people, processes, and technology, the UK National Cyber Security Centre (NCSC) developed the Cyber Assessment Framework (CAF). The framework is a structured approach developed by the UK National Cyber Security Centre to help organisations understand and assess their ability to manage cyber security risks. It provides a set of outcomes-focused principles that enable organisations particularly those responsible for essential services and critical infrastructure to evaluate whether their cyber security measures are effective in protecting against, detecting, responding to, and recovering from cyber threats. Rather than focusing on specific technologies, the CAF emphasises governance, risk management, resilience, and continuous improvement.

Quorum Cyber's Solution

The Quorum Cyber, Cyber Resilience Assessment (CRA) uses the NCSC CAF to evaluate, identify and understand your cybersecurity resilience, associated risks, and capabilities. It focuses on assessing the ability to manage cyber risk and maintain operational resilience during and after a cyber incident.

The CRA will focus on four primary objectives:

- Managing security risk,
- Protecting against cyber-attacks,
- Detecting cyber incidents,
- and minimising the impact of cyber incidents.

Each objective is assessed against defined principles and outcomes to determine how effectively resilience is embedded across people, process, and technology.

The assessment helps in identifying weak spots in resilience and risk, developing a roadmap for improvements, and demonstrating commitment to cybersecurity to your stakeholders.

The outcome of the assessment is comprehensive, business-aligned evaluation with a series of recommendations which align to the risk appetite of the organisation.

Unlike a maturity assessment, the CRA evaluates how the organisation performs under adverse cyber conditions.

Differentiators

The Quorum Cyber, Cyber Resiliency Assessment (CRA) delivers a comprehensive, business-focused evaluation of your organisation's security posture, highlighting areas of vulnerability and assessing how effectively systems can withstand and recover from current cyber threats.

Quorum Cyber's Cyber Resiliency Assessment is underpinned by a structured, outcome-driven framework aligned to the NCSC Cyber Assessment Framework's (CAF) risk-based objectives.

Service Features

The objective of this type of engagement is to ascertain the activities required to support your organisation in developing your cyber resilience over time, while acknowledging the organisations culture, working methods, and ethos.

Our methodology delivers a clear journey, enabling you to track progress against tangible security improvements along the way. This way, you can have a regular sense check of your investment, measuring its impact on your security posture.

This approach also empowers you to adapt to the ever-evolving threat context. What we know today is not what we will know tomorrow.

The Cyber Resiliency Assessment is delivered in the following stages:

- Understand Current Threat
 - An assessment to identify your most pertinent cyber-threats.
 - Threat profile your organisation.
- Understand Current Resilience
 - Business focused workshops to understand your business and resilience strategy. Business focused workshops to understand your business, risk, and resilience strategy.
 - A process and technology focused workshops to learn about how you work towards the objectives.
- Assessment
 - Measure resilience against NCSC CAF objectives.
 - Define the potential gaps between threats and processes.

The resulting assessment report includes:

- Executive-Level Summary – Clear, concise reporting designed for the C-suite and board, providing visibility of cyber resilience at a strategic level.
- Maturity-Aligned Insights – Direct linkage between resilience improvements and risk scores to support directed improvement.
- Clear Risk Ownership – Defined accountability for risks and remediation actions across the organisation.
- Informed Decision-Making – Enables leadership to make confident, evidence-based decisions grounded in business impact.
- Prioritised Investment Focus – Supports the prioritisation of security initiatives and investment in resilience improvements based on measurable risk reduction and recovery capability.

Service Benefits

By partnering with Quorum Cyber to complete a Cyber Resiliency Assessment underpinned by the NCSC Cyber Assessment Framework (CAF) the following benefits can be realised:

- **Clear Understanding of Cyber Resilience**
Provides a structured view of how well the organisation manages cyber risk across governance, protection, detection, response, and recovery.
- **Risk-Based Prioritisation**
Identifies gaps against outcome-focused principles, enabling organisations to prioritise improvements based on risk and business impact rather than technical detail.
- **Executive-Level Insight and Accountability**
Translates cyber security into business outcomes, enabling informed decision-making, clearer ownership, and stronger governance at senior leadership level.
- **Regulatory and Assurance Readiness**
Supports compliance with the UK Regulations and helps demonstrate due diligence to regulators, customers, and stakeholders.

Commented [DM1]: 3-10 benefits of the service.

What impact does this have on the customer?

What is the value it delivers?

What will this change for the customer?