Quorum Cyber

Service Description Cyber Security Risk 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

In an environment of escalating cyber threats, increasing regulatory scrutiny, and growing digital dependence, a Cyber Security Risk Assessment is a critical business activity rather than a purely technical exercise. It provides leadership with a clear, evidence-based understanding of the organisation's cyber risk exposure and the potential impact on strategic objectives, operations, reputation, and financial performance.

A Quorum Cyber Security Risk Assessment provides security leaders with a clear, objective view of their organisation's cyber risk landscape to support informed strategic focus and prioritisation. The assessment identifies and evaluates risks to critical assets, information, and services, replacing fragmented and inconsistent practices with a structured, repeatable, and business-aligned approach to managing cyber risk.

Quorum Cyber's Solution

Quorum Cyber's Security Risk Assessment service evaluates an organisation's cybersecurity practices, controls, and processes through a risk-focused lens aligned to recognised methodologies such as the NIST Risk Management Framework (RMF) and ISO/IEC 27005. The assessment identifies and analyses risks to critical assets, information, and services, highlighting areas of exposure and control effectiveness across governance, protection, detection, response, and recovery. This provides organisations with a clear, structured understanding of their cyber risk profile and preparedness to manage potential threats and incidents.

The insights from the assessment enable organisations to strengthen resilience by prioritising risk treatment activities, improving regulatory and assurance alignment, and optimising the allocation of resources based on risk impact. The service delivers practical, actionable recommendations and a prioritised risk treatment roadmap to support informed decision-making, improve operational effectiveness, and embed a sustainable, risk-based approach to cyber security aligned with business objectives.

Differentiators

By partnering with Quorum Cyber on a Security Risk Assessment, organisations gain access to our Centre of Excellence and deep cybersecurity expertise. Our team applies recognised risk management methodologies, including the NIST Risk Management Framework (RMF) and ISO/IEC 27005, to deliver a rigorous, evidence-based assessment that provides confidence in the findings and supports the development of targeted risk treatment recommendations and practical remediation roadmaps.

This approach goes beyond simply identifying control gaps, focusing instead on understanding and prioritising cyber risk in line with your organisation's risk appetite and business objectives. The value of the engagement lies in clear, actionable outcomes providing transparency into where risks exist, how effectively they are managed, and a structured, risk-based path to reducing exposure and strengthening organisational resilience.

Service Features

- Comprehensive Posture Evaluation,
- Risk prioritisation,
- Direction towards preparedness and readiness,
- Regulator support,
- Actionable insights and roadmap,

Service Benefits

- Clear Understanding of Organisational Cyber Risk
  Provides a structured view of risks to systems, data, and services, enabling leadership to understand where the most significant exposures exist and why they matter to the business.

- Stronger Governance and Risk Ownership
  Establishes clear accountability for risk decisions, including risk acceptance and treatment, supporting informed oversight by senior leadership and risk committees.

- Improved Alignment Between Security and Business Objectives
  Ensures cyber security activities are driven by risk and business impact rather than technical controls alone, enabling more effective prioritisation and investment decisions.

- Enhanced Regulatory and Assurance Readiness
  Supports compliance with regulatory and assurance requirements by demonstrating a structured, auditable approach to risk management and control effectiveness.

- Continuous Risk Management and Resilience Improvement
  Embeds an ongoing, lifecycle-based approach to managing cyber risk, enabling organisations to adapt to evolving threats and strengthen resilience over time.