Quorum Cyber

Service Description
Cyber Security Programme Review
G Cloud 15

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

Table of Contents

Service Overview

Background

Quorum Cyber's Programme Review service evaluates how effectively key security and resilience programmes are designed and operating to support the organisation's ability to withstand and recover from disruption. It focuses on critical areas such as Business Continuity and Disaster Recovery (BCP/DR) ensuring plans are practical, well-governed, and capable of sustaining essential services during major incidents and Identity and Access Management (IAM), which governs who can access systems and information and under what conditions.

The assessment considers whether these programmes align with recognised best practices and the organisation's resilience objectives, rather than simply whether policies or plans exist. By identifying strengths, gaps, and areas for improvement, it provides leadership with clear insight into how well these capabilities protect the organisation, where investment should be prioritised, and how resilience can be strengthened in a measurable and sustainable way

Quorum Cyber's Solution

Quorum Cyber's assessment service provides a structured review of Business Continuity and Disaster Recovery (BCP/DR) and Identity and Access Management (IAM) to help organisations understand how well they are prepared to withstand disruption and protect access to critical systems and information. The assessment examines whether continuity plans are realistic, clearly owned, and capable of supporting essential services during an incident, alongside how effectively access to systems and data is controlled, managed, and monitored. This approach highlights areas of strength and exposure, giving organisations a clear, practical view of their readiness to respond to operational, cyber, or service-impacting events.

The outcomes of the assessment are designed to support informed decision-making at a business level. Organisations receive clear, actionable recommendations that prioritise improvements based on impact and practicality, helping leadership focus investment where it will most strengthen resilience. By improving continuity planning, recovery capability, and access control, the assessment supports reduced operational risk, clearer accountability, and greater confidence that critical services, data, and people are protected when it matters most.

Differentiators

By partnering with Quorum Cyber on a Business Continuity, Disaster Recovery, and or Identity & Access Management review, organisations gain access to our Centre of Excellence and a consulting team with deep, practical expertise in resilience, incident response, access governance, and operational risk management. Our consultants combine experience in business continuity planning, crisis management, identity and access control design, and real-world incident response to deliver a rigorous, evidence-based assessment that provides confidence in the findings and supports the development of clear, targeted improvement plans.

This approach goes beyond simply identifying gaps in plans or controls. It focuses on how effectively continuity arrangements and access management practices support the organisation's critical services, people, and business priorities. The engagement delivers clear, actionable outcomes providing visibility into where resilience and access risks exist, how well they are managed in practice, and a structured path to strengthening preparedness, reducing exposure, and improving organisational resilience.

Service Features

- **End-to-End Continuity Review:** Assessment of business continuity and disaster recovery plans to confirm they are practical, up to date, and capable of supporting critical services during disruption.
- **Critical Service and Dependency Analysis:** Identification of essential services, systems, and third-party dependencies to ensure recovery priorities and tolerances are clearly defined and achievable.
- **Access Governance and Control Review:** Evaluation of how user access is granted, managed, and removed, ensuring appropriate controls are in place to protect sensitive systems and information.
- **Incident and Recovery Readiness Assessment:** Review of how continuity plans and access controls support effective response during cyber incidents, outages, or operational crises.
- **Evidence-Based Findings and Recommendations:** Clear identification of strengths, gaps, and risks, supported by practical recommendations aligned to business needs rather than technical complexity.
- **Actionable Improvement Roadmap:** Delivery of a prioritised roadmap to strengthen resilience, reduce operational risk, and improve confidence in continuity and access management capabilities.

Service Benefits

- **Improved Organisational Resilience**: Greater confidence that critical services can continue or recover quickly during disruption, reducing the impact of incidents on operations and service delivery.
- **Reduced Risk of Unauthorised Access**: Stronger control over who can access systems and data, lowering the risk of misuse, fraud, or security breaches.
- **Clearer Accountability and Governance**: Defined ownership and responsibilities for continuity and access controls, supporting better oversight and decision-making.
- **Prioritised Investment and Improvement**: Clear insight into where improvements will have the greatest impact, enabling more effective use of time, budget, and resources.
- **Increased Confidence for Stakeholders**: Demonstrable assurance to customers, partners, and regulators that the organisation is prepared, well-managed, and resilient.