

Service Description Enterprise AI Governance Workshop 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	3
Service Features	4
Service Benefits	5

Service Overview

Background

Organisations adopting Microsoft 365 Copilot face a significant risk: Copilot can only be as secure as the data, permissions, and controls that are in place. Poor data hygiene, over-permissive sharing, weak classification, and excessive content retention increase the likelihood that Copilot will surface sensitive, outdated, or inappropriate information to users. Many organisations lack visibility into where sensitive data resides, how it is shared, and whether existing Microsoft security and compliance capabilities are being fully utilised, creating both security exposure and reduced Copilot effectiveness

Quorum Cyber's Solution

The Quorum Cyber M365 Copilot Readiness Assessment is a structured, security- and compliance-led engagement that evaluates an organisation's readiness to safely adopt Microsoft 365 Copilot. It combines configuration reviews, Microsoft 365 sensitive data discovery, and maturity scoring against Microsoft best practices to identify risks, prioritise remediation, and provide a clear roadmap for secure Copilot enablement. The service delivers both executive-level insight and actionable technical recommendations to improve readiness and long-term posture

Differentiators

- **Security-first Copilot adoption:** Focuses on preventing data overexposure rather than just enabling Copilot features.
- **Deep Microsoft alignment:** Built on Microsoft Copilot readiness guidance and advanced use of Purview, Defender, Entra ID, and eDiscovery capabilities.
- **Data-driven risk analysis:** Goes beyond configuration checks to analyse real customer data, containers, and sharing patterns.
- **Maturity-based scoring model:** Clear "current vs future" maturity view to support prioritisation and investment decisions.
- **Operational realism:** Recommendations consider existing licensing (e.g. E5), in-flight initiatives, and organisational constraints.
- **Knowledge transfer included:** Upskills internal teams to sustain readiness as Copilot evolves

Service Features

- Kick-off & scoping workshop to confirm objectives, prerequisites, and delivery approach.
- Current-state security and compliance evaluation of Microsoft 365 data security configurations against best practice.
- Sensitive data assessment using Microsoft eDiscovery and built-in Sensitive Information Types across SharePoint, OneDrive, and Exchange.
- SharePoint & Teams container risk analysis, scoring sites based on age of content, sensitivity, external sharing, privacy settings, and labelling.
- Copilot readiness maturity scorecard, covering preparation, permissions, classification, protection, and lifecycle management.
- Assessment of Purview, DLP, retention, and labelling capabilities, highlighting underutilised controls.
- Executive summary and detailed technical report with prioritised findings and recommendations, including implementation roadmap.
- Knowledge transfer sessions to support secure Copilot adoption and future feature enablement

Service Benefits

- Reduced risk of sensitive data exposure via Copilot and Microsoft Search.
- Improved Copilot response quality, driven by better data hygiene, relevance, and lifecycle management.
- Clear visibility of high-risk data locations and sharing practices across the tenant.
- Stronger security and compliance posture, aligned to Microsoft and regulatory best practices.
- Actionable roadmap to move from current to target maturity using existing Microsoft investments.
- Greater confidence enabling Copilot at scale, with controls embedded by design rather than retrofitted later