



Microsoft Copilot Readiness Assessment (M365)

Service Description

G Cloud 15



Contents

Introduction 2

Service Description 3

 Who this service is for 3

 What the service does 3

Deliverables 5

 Benefits 5

 Inputs required from the customer 5

 Service constraints 5

Microsoft Copilot Packages and Value Alignment 6

Onboarding process 7

 Timescales 7

 Service location 7

 Data handling and security 7

Why UK Public Sector Organisations benefit when they Partner with Ekco Cloud & Security 8

 Security-First Cloud Services Aligned to Government Standards 8

 End-to-End Capabilities Mapped to G Cloud 15 8

 Scalable Expertise and Sovereign Delivery 8

 Tailored Solutions for Resource-Constrained Organisations 8

 AI-Enhanced Security Operations 9

 Public Sector-Focused Engagement Model 9

 Global Recognition and Strategic partnerships 9



Introduction

Ekco Cloud & Security is an ideal partner for public sector organisations seeking a **secure, compliant, and scalable provider** via G Cloud 15.

We make it easier for IT teams to innovate, scale, manage, troubleshoot and secure. Across cloud, business continuity, security and workspace solutions, we enable the growth our customers want with the team they already have.

Through our security-first approach, large specialist workforce, AI-enhanced operations, and proven delivery capability, we help organisations:

- Modernise securely
- Strengthen cyber resilience
- Reduce operational risk
- Improve service continuity
- Deliver safer, more reliable digital services for our customers and their stakeholders.

Ekco's end-to-end cloud and cyber services are well matched to **G Cloud purchasing needs and public sector transformation goals**.

Service Description

Microsoft Copilot is a strategic capability that can deliver significant productivity, automation, and security benefits across the public sector when deployed safely and responsibly. However, Copilot's value is directly dependent on the underlying Microsoft 365 configuration, data governance, and security posture of the tenant in which it operates.

The Microsoft Copilot Readiness Assessment provides public sector organisations with an independent, evidence-based view of their preparedness to adopt Copilot. It evaluates technical readiness, data access controls, information governance, and AI usage safeguards to ensure Copilot can be enabled without increasing the risk of data oversharing, non-compliance, or unintended access to sensitive information.

This assessment also aligns readiness outcomes to the latest Microsoft Copilot licensing and packaging models (as of 2026), enabling organisations to make informed decisions on which Copilot packages deliver the most value for their operating model, risk profile, and maturity level. The result is a clear, prioritised roadmap that supports safe adoption, phased rollout, and confident procurement decisions.

Who this service is for

This service is suitable for public sector organisations that:

- Use Microsoft 365 and are considering Microsoft Copilot adoption
- Operate in regulated or sensitive environments (for example legal, justice, finance, or healthcare)
- Require assurance over data access, security, and governance before enabling AI tools
- Need an independent readiness assessment prior to pilot or full rollout

What the service does

The service delivers a structured readiness assessment across four core areas:

1. Tenant configuration and licensing

- Review of Microsoft 365 tenant configuration for Copilot compatibility
- Validation of Microsoft 365 licensing (E3/E5 and Copilot add-on readiness)
- Review of identity and access controls, including MFA and Conditional Access
- Assessment of legacy authentication exposure
- Review of Copilot feature configuration, approved apps, and plugins

2. Data access and collaboration controls

- Review of OneDrive, SharePoint, Teams, and Microsoft 365 Groups access models

- Identification of oversharing risks (internal and external)
- Review of guest access and external sharing settings
- Assessment of device compliance and endpoint controls (Intune-managed devices)
- Review of grounding data access used by Copilot

3. Data governance and compliance

- Review of sensitivity labels and retention labels
- Assessment of label application and enforcement
- Review of Data Loss Prevention (DLP) policies relevant to Copilot usage
- Review of audit logging and monitoring configuration
- Assessment of legal hold considerations for Copilot-generated content

4. AI governance and usage controls

- Review of existing AI usage or governance policies (if available)
- Assessment of approved and restricted Copilot use cases
- Consideration of human-in-the-loop controls and privilege handling
- Review of AI output controls such as disclaimers or footers

Deliverables

Customers receive the following deliverables:

- A Copilot Readiness Assessment report
- A gap analysis identifying risks and non-compliance areas
- Prioritised, actionable recommendations to remediate identified gaps
- A remote read-out session to explain findings and next steps

Benefits

- Reduced risk of data oversharing or information leakage when using Copilot
- Clear understanding of technical and governance readiness
- Independent assurance prior to enabling AI capabilities
- Actionable roadmap for safe and compliant Copilot adoption

Inputs required from the customer

To deliver the service, the customer must provide:

- Read-only administrative access to relevant Microsoft 365 admin portals
- Access to existing documentation (where available), such as information protection or AI policies
- A technical contact to answer clarification questions during the assessment

Service constraints

- The service is advisory only and does not modify the customer environment
- Findings are based on the configuration at the time of assessment
- The service assumes the Microsoft 365 tenant remains stable during delivery
- Further Professional Services can be engaged to implement, modify and manage the customers' environment

Microsoft Copilot Packages and Value Alignment

This assessment aligns Copilot readiness activities with the latest Microsoft Copilot licensing and packaging models to ensure organisations select the most appropriate and cost-effective options while maximising value and maintaining compliance. As of January 2026, Microsoft Copilot capabilities are delivered through several complementary packages, each targeting different organisational needs.

- Microsoft 365 Copilot (Enterprise): A paid add-on to Microsoft 365 E3/E5 and equivalent plans, providing deep Copilot integration across Word, Excel, PowerPoint, Outlook, Teams, Copilot Chat, Pages, Notebooks, and internal agents via Copilot Studio.
- Microsoft 365 Copilot Business: Introduced in December 2025 for organisations with up to 300 users, offering the same Copilot experience at a lower price point and supporting phased, role-based adoption.
- Copilot Studio: Available as part of Microsoft 365 Copilot for internal agents or as a standalone, consumption-based service for advanced automation and external-facing agents.
- Microsoft 365 E5 with Security Copilot: Microsoft 365 E5 now includes Security Copilot, enabling AI-assisted threat investigation, incident response, and security operations across Microsoft Defender, Entra, Intune, and Purview.
- Microsoft Fabric with Copilot: Copilot is available from Fabric F2 SKUs upwards, enabling natural-language analytics, Power BI report generation, and data exploration.

Onboarding process

1. Service initiation and scheduling
2. Access provisioning and documentation review
3. Remote assessment and analysis
4. Report production
5. Findings and recommendations review meeting

Timescales

The service is typically delivered within **2–4 weeks**, depending on tenant size, complexity, and access availability.

Service location

The service is delivered remotely.

Data handling and security

- No customer data is extracted, copied, or retained
- Assessment activities are limited to configuration review and metadata inspection
- Access is read-only and time-bound
- All activities align with UK public sector security expectations

Why UK Public Sector Organisations benefit when they Partner with Ekco Cloud & Security

Security-First Cloud Services Aligned to Government Standards

Ekco Cloud & Security is a leading UK and European **security-first managed cloud provider**, delivering deep expertise across cyber security, identity, and cloud. Our services align with **NCSC guidance, the Cyber Assessment Framework (CAF), NHS DSPT**, and wider public sector assurance requirements. Our proven **Assess → Protect → Detect → Respond** model supports secure-by-design digital transformation across hybrid and distributed environments—directly addressing public sector risk and resilience priorities.

End-to-End Capabilities Mapped to G Cloud 15

Public sector buyers need suppliers that can deliver migration, protection, management, and optimisation through a single, accountable partner. We provide a **fully integrated cloud and security portfolio**, including:

- Cloud migration and managed cloud operations
- Security and infrastructure management
- Identity security and privileged access management
- Secure modern architecture design
- Real-time threat detection and incident response

These services align directly with **G Cloud 15 lots and purchasing criteria**, enabling organisations to modernise securely while managing complex legacy estates.

Scalable Expertise and Sovereign Delivery

With **1,000+ cloud and security specialists across the UK and Europe**, we offer the scale, depth, and resilience required to support mission-critical public services. A dedicated **identity security practice** provides mature capability for access control and Zero Trust adoption—an increasingly critical requirement across government organisations.

Tailored Solutions for Resource-Constrained Organisations

Recognising the challenges faced by councils, NHS trusts, education, and blue-light services, we offer **cost-effective, scalable cloud and cyber security solutions** designed for organisations with limited internal capacity.

These services protect against phishing, ransomware, and social engineering while meeting G Cloud's expectations for solutions that are secure by default, rapidly deployable, and low overhead.

AI-Enhanced Security Operations

We embed **AI into daily security operations**, improving analyst productivity and response effectiveness. AI-assisted services accelerate:

- Incident triage and prioritisation
- Threat analysis and vulnerability summarisation
- Reporting accuracy and audit readiness

This enables faster outcomes and stronger protection for public bodies operating with limited staffing.

Public Sector-Focused Engagement Model

Our partnership-led approach aligns with government procurement expectations, offering:

- Dedicated, accountable delivery teams
- Transparent SLAs and service reporting
- 24/7 support with local expertise
- Predictable commercial and contract models

This ensures we act as a **strategic long-term partner**, not a transactional supplier.

Global Recognition and Strategic partnerships

These global accreditations partnerships show our commitment to customer satisfaction, data safety, security and overall quality. We're independently audited every year to give our customers confidence in our approach.



From agile managed cloud platforms to next-gen security services that supercharge defences, our local team of specialists provide proactive, round-the-clock management. With one Ekco Cloud & Security team delivering a combination of services, our customers quickly gain control and visibility over their technology.