# Copilot Security Readiness

## Status: Early Planning - Q4 2025

**Expected Duration:** 6-8 weeks  
**Target Audience:** Organizations planning Copilot deployment  
**Prerequisites:** Sensitivity Labelling Uplift, Basic DLP Advisory

## Purpose & Problem Solved

Microsoft Copilot’s AI capabilities create new security and compliance considerations around data exposure, content generation, and information governance. Organizations need to prepare their data landscape and implement appropriate controls before enabling AI-powered productivity tools.

This engagement ensures Copilot deployment occurs within a secure, compliant framework that protects sensitive information while enabling the productivity benefits of AI assistance.

## Expected Deliverables

* Copilot readiness assessment across data governance and security controls
* Data classification review and enhancement for AI scenarios
* DLP policy optimization for AI-generated content
* Information barriers configuration for AI-assisted collaboration
* Privacy impact assessment for AI data processing
* User training framework for secure AI adoption
* Monitoring and compliance procedures for AI usage
* Risk mitigation strategies for AI-specific threats

## Integration with E2 Portfolio

**Natural Progressions:** - Sensitivity Labelling Uplift → Copilot Security Readiness (classification enables AI controls) - Basic DLP Advisory → Copilot Security Readiness (prevents AI data leakage) - Data Security Audit → Copilot Security Readiness (baseline governance for AI) - Copilot Security Readiness → AI Governance Program (future module)

**Complementary Services:** - Information Barriers Implementation (future module) - Advanced Privacy Controls (future module)

## Key Focus Areas

* **Data Preparation:** Ensuring appropriate classification and governance for AI processing
* **Privacy Protection:** Controls for sensitive data exposure through AI interactions
* **Content Controls:** Managing AI-generated content creation and sharing
* **User Guidance:** Training for secure and effective AI tool usage
* **Compliance Alignment:** Meeting regulatory requirements in AI-enabled environments
* **Risk Assessment:** Understanding and mitigating AI-specific security risks

## Express Early Interest

Contact Engage Squared to participate in early market research and help define engagement scope.

**Contact:** E2 AI and Security Practice  
**Market Research:** Participating in customer needs assessment for AI security