# Agent Governance & Assurance Uplift

## Overview

The **Agent Governance & Assurance Uplift** is designed to provide customers with confidence that they have the right level of **visibility, control, and governance maturity** in place for Microsoft Copilot agents. The offering ensures organisations can answer three critical questions:

1. **Who is building agents?** (Visibility)
2. **What data and systems can those agents access?** (Controls)
3. **Where and how are those agents managed across their lifecycle?** (Governance)

This engagement delivers both **operational guardrails** and an **executive-level assurance snapshot**, helping clients balance innovation with control.

## Objectives

* Establish a baseline of existing agent governance maturity.
* Provide visibility into the current state of agent creation, environments, and controls.
* Identify governance gaps against a structured zone model (Safe → Supported → IT Managed).
* Recommend uplift actions across people, process, and technology.
* Deliver an assurance snapshot that can be shared with business and executive stakeholders.

## Scope

The engagement focuses on four key areas:

1. **Discovery & Baseline**
   * Inventory of Retrieval, Personal, and Crucial Agents.
   * Review of governance artefacts (policies, admin centre usage, conditional access, DLP, CoE reports).
   * Map current practices against the Zone Strategy (Safe, Supported, IT Managed).
2. **Gap Assessment**
   * Visibility: Is there oversight of agent creation and usage?
   * Controls: Are risky connectors restricted? Is cost monitoring enabled?
   * Lifecycle: Are there processes for testing, deployment, monitoring, and retirement?
   * Language: Is “governance” framed in business-friendly terms (operating models, service management)?
3. **Uplift Roadmap**
   * **Quick Wins**: Enable auditing, activate CoE dashboards, restrict high-risk connectors.
   * **Mid-Term**: Formalise approval workflows, introduce Dev/Test/Prod separation for high-value agents.
   * **Long-Term**: Integrate into enterprise change management, embed in broader SDLC/DevSecOps frameworks.
4. **Assurance Snapshot**
   * Maturity rating (Low, Developing, Established, Advanced).
   * Heatmap of coverage across Visibility, Controls, Lifecycle, and Governance.
   * Priority recommendations by zone (Safe, Supported, IT Managed).
   * Executive-ready one-page summary to provide assurance.

## Deliverables

* **Discovery Report**: Inventory of current agents, environments, and controls.
* **Governance Gap Assessment**: Detailed findings mapped to the zone model.
* **Uplift Roadmap**: Phased actions across quick wins, mid-term, and long-term improvements.
* **Assurance Snapshot**: A concise, executive-friendly summary of governance maturity and next steps.

## Outcomes

* Improved **visibility** into who is building agents and where.
* Greater **confidence** that controls exist for agent access, cost, and data governance.
* Alignment of **agent lifecycle** with secure software development and IT processes.
* Executive-level **assurance** that proliferation risks are managed and innovation remains safe.

## Engagement Approach

* **Duration**: 4–6 weeks (flexible depending on client scope).
* **Format**: Combination of workshops, stakeholder interviews, and technical assessments.
* **Participants**: Business stakeholders, IT admins, makers, security teams.
* **Tools**: Microsoft Admin Centers, Power Platform CoE Starter Kit, governance dashboards.

## Useful Links

* [Power Platform Center of Excellence (CoE) Starter Kit](https://aka.ms/coestarterkit) A Microsoft-maintained, open-source toolkit that provides dashboards, apps, and flows to help organisations gain visibility and enforce governance across Power Platform. It is a key enabler for discovering agent usage and monitoring proliferation.

## Next Steps

* Run a **discovery workshop** with client stakeholders.
* Deploy or review CoE dashboards for initial visibility.
* Assess agent proliferation risks across the three zones.
* Present Assurance Snapshot and Uplift Roadmap to executive sponsors.