

COPILOT STUDIO COMPUTER USE EXPANDS DESKTOP CONTROL BEYOND DEVELOPERS

OPERATIONAL SIGNAL

DOMAIN: CAP — Capability | **CONFIDENCE LEVEL:** Preliminary

INSTITUTIONAL DIMENSIONS: Authority | Attribution | Visibility | Escalation | Continuity

Signal ID	Platform	Source	Audience	Status	Date
SIG-CAP-009	Microsoft Copilot Studio	Link	PMO Risk Ops IT	Pilot	2026-06-08

CAPABILITY SHIFT

Microsoft Copilot Studio now allows agents to automate web and desktop applications by controlling browsers and applications on behalf of users. Computer use lets an agent see what is on screen, move a cursor, click, type and navigate between applications. Copilot Studio is a low-code platform used by business users, citizen developers and IT teams. The release also includes related governance features, including Entra agent identities, agent inventory and an agent readiness page.

ORGANISATIONAL CONSEQUENCE

Computer use is no longer only a developer-facing agent capability. Business users with Copilot Studio access may be able to build agents that operate through web or desktop interfaces. The agent may not need API access if it can use the visible application interface. Controls designed around files, APIs or connected data sources may not fully describe this operating mode.

WHAT TO WATCH

- Agents using web or desktop applications
- Business users building screen-control agents
- Agents operating internal or client-facing systems
- Desktop actions that look like ordinary user activity

WHY THIS MATTERS NOW

Computer use in Copilot Studio is generally available, while some related governance tooling is in preview or requires configuration. The issue is no longer only what agents can do, but who can build them.

WHAT TO REVIEW

- Whether Copilot Studio computer use is enabled or restricted
- Who can build agents with desktop control
- Whether agent identities and inventory are configured
- How agent actions appear in audit records
- Guidance for agents using internal or client-facing systems

GOVERNANCE CONTEXT

This is an authority and visibility issue. Computer use shifts agent activity into the same interface people use to perform work. Existing controls may describe data access, but not screen-level action through business applications.

Scope Boundary: This artefact translates observed platform capability changes into operational considerations. It does not constitute policy, legal advice, or enforcement guidance.