

Copilot Studio Governance Baseline

A sequenced planning reference for Microsoft 365 Copilot and Copilot Studio agents: ownership and data boundaries, delivery, publishing, evidence, and consumption.

Early planning can help

Personal, read-only productivity agents can use a low-risk lane. Shared, action-taking, or mission-critical agents may benefit from an IT-managed lifecycle. Each organization can define its own classifications, approvals, ownership fields, and review cadence.

PHASE 1 FOUNDATION Establish control	PHASE 2 DELIVERY Release safely	PHASE 3 OPERATIONS Publish and sustain
1 Classify and assign owners Consider whether an agent is personal, departmental, or mission-critical. Helpful ownership details can include business and technical owners, a backup, support contact, audience, risk, cost center, and review date. Governance zones >	4 Review data and connections Before connecting SharePoint, consider reviewing its permissions. It can also help to record sources, endpoints, connection identities, secrets, third-party processors, and residency exceptions, and to evaluate user-context access. SharePoint knowledge access >	7 Gate sharing and publishing Editor and Viewer access can be separated and scoped to selected users or groups. Organizations may include owner, security/data, test, support, or funding review before broad publishing. GCC organization-wide publication uses admin submission. Share agents safely >
2 Create lifecycle environments Separate development, test, and production environments can help isolate shared agents. Entra security groups, group-team roles, and limited production authoring access are controls an organization can consider. Environment strategy >	5 Standardize build and test Useful test planning can include clear instructions, reviewed tools, safe failure behavior, expected outcomes, abuse cases, a support path, and test evidence. Limited-user validation can provide feedback before broader release. Test your agent >	8 Monitor, retain, and respond In supported Dataverse environments, settings can control transcript saving and owner/editor access; Power Apps viewing also requires Bot Transcript Viewer. M365 Copilot agents don't write to this table. Purview controls are available in GCC subject to licensing. Transcript controls >
3 Enforce DLP and identity Microsoft Entra authentication and data policies can help govern knowledge types, connectors and tools, HTTP, skills, and channels. Endpoint filtering is preview and can be evaluated in GCC. Testing policies before publishing can confirm expected behavior. Configure data policies >	6 Promote with controlled ALM Custom solutions can support moving agents between environments. Teams can review required objects before export and plan for target-specific component and authentication setup after import. PAC CLI and Azure DevOps Build Tools support GCC. Solutions and ALM >	9 Fund, meter, and review It may be useful to identify a capacity owner, cost center, and funding path for each production environment. PAYG and newer capacity controls can be confirmed in the target GCC tenant. Billing configuration guide >

Possible production-readiness checks

✓ Primary and backup owners	✓ Approved audience and risk	✓ Entra authentication	✓ DLP policy passes
✓ Versioned solution release	✓ Security and UAT evidence	✓ Support and incident path	✓ Funding and overage decision

Billing and capacity reference

Verify conditional controls in the target GCC tenant.

Copilot Studio billing paths, allocation options, overage behavior, and Azure cost alerts are explained in the [Copilot Studio Billing Configuration Guide >](#)