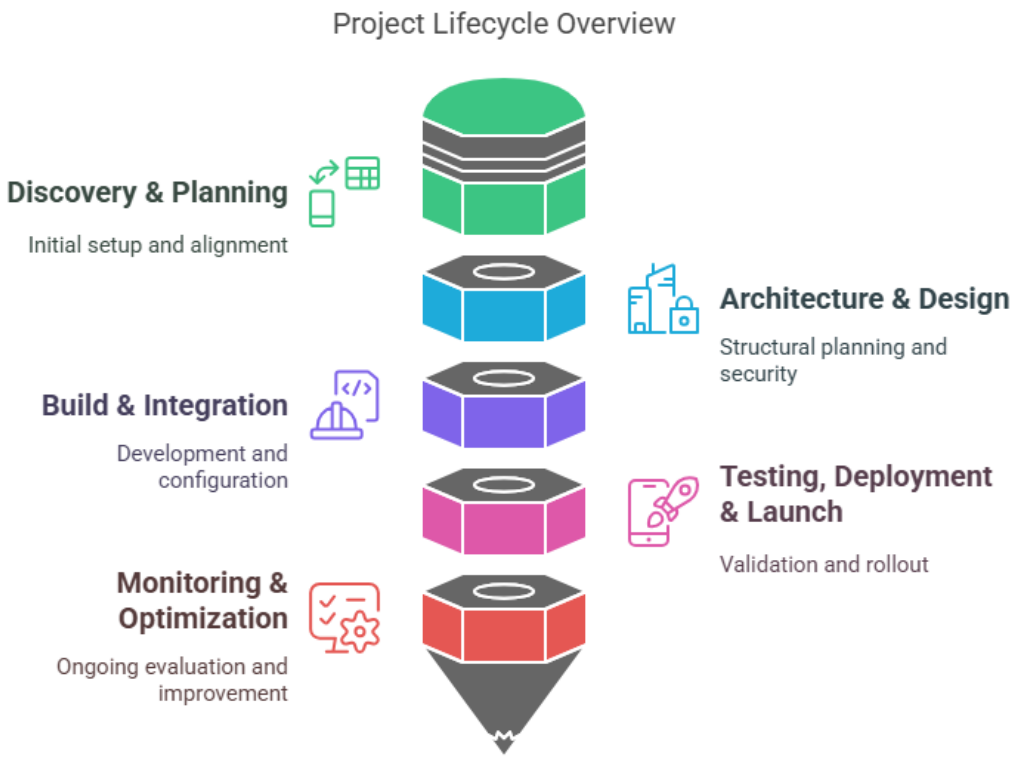
Copilot Studio Governance & Security Guide

Overview

The purpose of this guide is to offer Copilot Agents admins, Copilot Studio COE leads, and other related stakeholders a concise governance and security guide for managing Copilot agents across their enterprises. It also aims to highlight the critical areas that should be considered in governing, securing, and monitoring Copilot agents.

How to use this guide

This guide divides Copilot Studio projects into five key phases, assisting administrators and operations teams in focusing on the relevant governance and security aspects of each phase. By examining the relevant project phase of your Copilot Studio you can review the pertinent sections and key areas for that specific phase.



Phase 1: Discovery & Planning

Initial Governance Requirements

- **Stakeholder Alignment:** Ensure the involvement of IT, Security, Compliance, and Legal departments from the outset. Establish and document the data residency, retention, and privacy policies that will guide the necessary governance and security features to be configured/enabled in your organization.
- **Compliance Review:** Outline and document the necessary regulations for your organization (GDPR, HIPAA) and detail your organization's data and transcript retention requirements.

Key Objectives, Business Scenarios, and Data Protection

- **Business Alignment:** Determine the target business scenarios and tasks that the Copilot Agent will address (e.g., responding to customer order inquiries) and identify the required systems and data integration to identify potential risks and implement necessary security measures.
- **Restricting Data Sources:** Document the existing knowledge and data sources within your organization that may be utilized by the Copilot Agent. Include compliance requirements and integration points such as SharePoint, Teams, and Dataverse in alignment with the business requirements, specifying if Agents will be permitted to use their own AI general knowledge.
- **Data Protection & Risk Assessment:** Classify the sensitivity of all documented data sources (e.g., general, confidential, etc.), evaluate the potential risks of data leakage associated with these data sources, and establish the necessary security and privacy policies to protect this data (e.g., blocking certain data source connectors and/or data sources), specifying data masking requirements in your organization to create and manage Power Platform masking rules accordingly.

Naming & General Guidelines

- **Copilot Agent Naming:** Implement agent naming conventions (e.g., "Contoso-CustomerServiceAgent") to facilitate the identification of various Copilot Agents within your organization.
- **Solution Naming Standard:** Implement a consistent naming convention for your Copilot Agent solution (e.g., "ContosoCopilot") to ensure proper encapsulation and deployment through your ALM pipeline, avoiding the accidental deployment of non-production solutions into the production environment.

- **Disclaimer Guidelines:** Document and share the conversation disclaimers and warnings template that must be included for each Copilot agent (e.g., in the conversation start topic) to ensure consistency and compliance with organizational standards.
- **Shared Components:** Identify any mandatory shared entities or reusable components (e.g. knowledge sources or Topics) to be used by all Copilot agents in your organization to ensure consistency and where you can leverage Copilot Studio component collections.

Licensing & Budget

- **License Assessment and Assignments:** Evaluate the M365, Power Platform, Dynamics 365, Copilot, or Azure licenses held by the organization to understand its current entitlements as this could potentially have implications on the type of additional licenses required to use premium features such as Enhanced search results and Managed Environment. Establish a policy within your organization to assign Copilot user licenses and manage access to copilot studio.
- **Cost Estimates:** Consider the cost implications of leveraging some of Gen AI and premium features such as premium connectors, managed environment and determine the billing model that best suits your organization (e.g., pay as you go vs. capacity licensing).
- **Allocate Message Capacity:** Assign capacity at an environment level by allocating "add-ons" to ensure that users within the designated environment have access to the specified Copilot Studio messaging capacity.

Relevant References & Resources

- Microsoft Copilot Studio Security & Governance
- Microsoft Power Platform Licensing Overview
- Security and governance - Microsoft Copilot Studio | Microsoft Learn
- Managed Environments overview - Power Platform | Microsoft Learn

Phase 2: Architecture & Design

Environment Strategy

- **Environment Isolation:** Build an environment strategy for your organization and maintain distinct environments for Development, Testing, and Production. Define Data Loss Prevention (DLP) policies for each environment and ensure that

each Copilot Maker uses their own Development environment for creating Copilot agents by enabling features such as environment routing.

- **ALM Process:** Implement a healthy application lifecycle management (ALM) process within your organization and build deployment pipelines for solution versioning and deployment automation using in-product pipelines or external DevOps platform such as Azure DevOps.

Security & Access Controls

- **Secure your tenant and environments:** Consider using and enabling features such as Lockbox, Dataverse audit, IP firewall, and IP cookie binding to secure your environments and tenant against attacks.
- **Network Security:** To minimize public exposure of any endpoints used by your Copilot agent, utilize Azure Private Link, firewalls, or service endpoints for the different used components of your Copilot and overall solution.
- **Conditional Access:** Apply Azure AD Conditional Access for corporate devices and networks.
- **Allowed Authentication:** Establish the permitted user authentication model for the Copilot agent within your organization (e.g., authentication via Entra ID vs. manual authentication or no authentication required). Additionally, decide on restricting or permitting Web Channel access to ensure an appropriate security level for your web channel.
- **Restricted User Access:** Consider limiting authoring access to Copilot Studio to specific security groups to control authoring privilege by leveraging security groups.

Data & Access Security

- **Geographic Data Residency:** Understand and evaluate the security and geographic data residency and location in Copilot Studio agents against the data residency and compliance requirements of your organization.
- **Role Based Access Control:** Administrators are advised to use Power Platform RBAC and leverage security groups to assign appropriate roles (e.g., admin, maker, or end-user) to each Copilot Studio user within the Power Platform admin center to ensure proper access management across all environments.
- **MFA & Identity:** Enable multi-factor authentication (MFA) for all Power Platform and Copilot users through Microsoft Entra ID across your entire environment to ensure secure access.

- **Least Privilege:** Restrict agent permissions to essential data sources and consider using a service principal account for production environment deployment and custom connector authentication.

Governance & DLP Considerations

- **DLP Policies:** Establish environment-level or tenant-level Data Loss Prevention rules for your agent to restrict unused first-party (1P) and third-party (3P) connectors (business versus non-business) based on the agent's use case and requirements.
- **Shared Connections:** Decide if Copilot agents will run actions in a user context or dedicated service account (Copilot author account) to properly manage the access permission of your Copilot Agent.
- **Sharing and Channel Control:** Enforce publishing channel restrictions to prevent unauthorized sharing and ensure all sensitive data is properly labeled in knowledge sources.

Generative AI Features

- **AI Orchestration Type:** Choose the appropriate orchestration type for your organization, selecting between classic and Generative orchestration based on your specific organizational and use case requirements.
- **Copilot Agent Types:** Determine the suitable agent triggers to be implemented within your organization, opting for either autonomous (trigger-based) or conversational agents based on your business scenarios and in accordance with your organization security policies.
- **Conversation Language Understanding Model:** Choose the language understanding model permitted for use in your organization. Decide between the default Microsoft Copilot Studio NLU or custom CLU based on your requirements, data complexity, and the available skillset within your team.

Relevant References & Resources

- Power Platform Environment Strategy
- Azure AD Conditional Access
- Information Barriers in Microsoft 365

Phase 3: Build & Integration

Solution & agent Development

- **Shared Components:** Ensure that the outlined disclaimer message, multi-language support, and required organizational components as per your organization guidelines are included in your Copilot agent implementation.
- **Custom instruction / Custom Prompts / AI Builder:** Ensure established custom instructions and prompt templates are implemented following your internal governance and guidelines (e.g., "don't include competitors' information in the response", "Your tone should be friendly", etc.).

Configuration & Connection Management

- **Connector / Connection Setup:** Validate permissible connectors / connections against DLP rules in each environment (Dev, Test, and Production) to ensure your Copilot agent is functioning properly across environments and that there are no missing dependencies or broken connection references.
- **Managed Environment & Environment Groups (Premium Feature):** Create an Environment Group for your solution's different environments and configure the policies of each environment group accordingly to ensure all used environments are properly secured. Refine tenant-wide DLP policies to align with project architectural needs and determine if specific tenant-wide DLP policies are required to block specific connectors to prevent data exfiltration.
- **Configure Agent-level settings:** Define each agent's orchestration model, channels, and language settings.
- **Errors and Warnings:** Ensure you pay attention to security warnings. Makers can view security alerts for their agent prior to publishing it when default configurations for security and governance are altered, and should use the topic checker to monitor for error messages and warnings.

Relevant References & Resources

- Power Platform DLP Policies

Phase 4: Testing, Deployment & Launch

Testing & Validation

- **Test Use Cases:** Leverage the Power CAT Copilot Studio kit for automated scenario testing (security, data integrity) to ensure proper use-case coverage of all your core scenarios including security and governance-related use cases.
- **CI/CD:** Run and test your automated deployment solution/pipeline with Azure DevOps or GitHub to maintain version control.
- **ALM Process:** Implement a healthy application lifecycle management (ALM) process within your organization and build deployment pipelines for solution versioning and deployment automation using in-product pipelines or external DevOps platform such as Azure DevOps.

Final Security & Compliance Checks

- **DLP & RBAC Validation:** Ensure environment-level policies, roles, and connections are correctly configured in the production environment and that the right DLP policies are enabled.
- **Azure Management:** Review and approve integrated app registration, VNets, keys, and endpoints in Azure for your production resources.
- **Production Knowledge Sources and Data:** Ensure that all production knowledge sources (e.g., SharePoint libraries) and production documents are properly referenced for production agents, especially if different ones were used during development and testing.

Production Rollout

- **Deployment:** Use your ALM pipeline for version control and to safely move your Copilot agent/solution across environments and ensure all dependencies are configured properly in your production environment.
- **Launch Strategy:** Communicate new Copilot Agent availability, usage disclaimers, and training for all your internal stakeholders.

Enable Monitoring & Governance

- **Telemetry Setup: :** Integrate Azure Application Insights for usage, performance, and error logging, and leverage AKV for key rotation when applicable.

- **Power Platform CoE Starter Kit :** Implement the Microsoft Power Platform Center of Excellence (CoE) Starter Kit to effectively monitor Copilot Agents throughout your organization.

Relevant References & Resources

- Power CAT Copilot Studio Kit
- Microsoft Power Platform Build Tools (Azure DevOps)
- Azure DevOps or GitHub Actions for Power Platform ALM
- Azure Application Insights for Copilot Studio
- Center of Excellence (CoE) Starter Kit

Phase 5: Monitoring & Optimization

Operational Monitoring

- **Analytics, Dashboards & Reports:** Utilize the Copilot Studio's built-in analytics dashboard to oversee agent usage and key performance indicators, identifying opportunities for enhancement. Additionally, take advantage of real-time telemetry from the agent and supplementary Microsoft tools such as Power BI and Application Insights to develop custom analytics for your organization.
- **Alerts & Incident Response:** Admins can monitor and receive alerts on agent activities through Microsoft Sentinel. To enable audit logging for Copilot Studio in Microsoft Sentinel ensure users have an assigned Microsoft 365 license and configure Microsoft Sentinel to ingest audit logs from Microsoft Purview. Use Microsoft Sentinel's analytics capabilities to create custom detection rules for Copilot Studio events. Admins should also leverage PPAC action center (Advisor) and Copilot center for recommendations and alerts.

Compliance & Auditing

- **Auditing & Threat Detection:** Track and Audit Copilot Studio activities, data modifications, user actions in Microsoft Purview.
- **Transcript Management:** Copilot Conversation transcripts are stored in the Dataverse Conversation transcripts table with a data retention period of 30 days. However, customers have the option to extend the retention period for conversation transcripts in Dataverse. If there is a requirement within your organization to retain conversation transcripts for a longer duration, it is recommended to export the raw

conversation transcripts data to a more cost-effective data store such as Azure Data Lake Storage Gen2 using the Azure Synapse Link for Dataverse feature.

- **Content Moderation:** View count of blocked queries as part of Responsible AI initiatives in Power Platform Admin center Copilot page.
- **Monitor Tenant, Environment, and Agent Security:** Leverage the Power Platform admin security page to streamline your governance through a unified experience with greater visibility and easily accessed controls, all in one place.

Continuous Improvement

- **User Feedback:** Gather input (Teams channels, surveys) to refine conversation flows, user experience, or security policies, and use the Copilot analytics dashboard to improve your Copilot agent.
- **Feature Updates & Innovation:** Pilot new Copilot features (e.g., advanced AI feature) in test environments before wider release.
- **Governance Reviews:** Reassess environment configurations, DLP settings, and compliance at least quarterly.

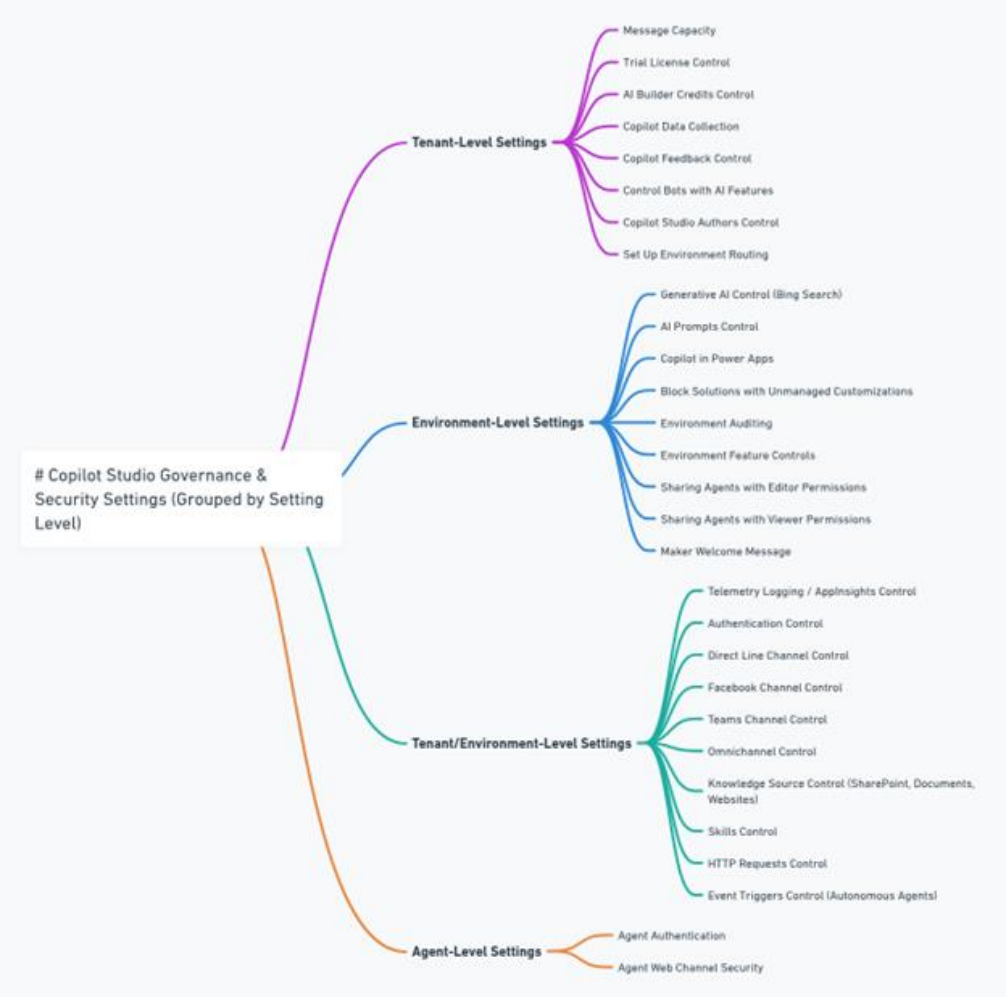
Usage and Capacity Management

- **Capacity & Quota Monitoring:** Monitor and manage your copilot agents' message usage and capacity and other solution dependencies (e.g., Power Automate, AI Builder, etc.) in Power Platform Admin Center to prevent overages and service throttling.

Relevant References

- Azure Monitor & Microsoft Sentinel
- Microsoft Purview Audit (Standard and Premium)
- Copilot Studio Security and Governance Documentation
- Microsoft Copilot Studio Security & Governance
- CoE Starter Kit Overview
- App Insights Overview
- Microsoft Purview Compliance Portal
- Power Platform Admin Center
- Related Copilot Governance & Security Configuration Settings

Key Copilot Configuration Settings



Tenant-Level Settings

Setting	Purpose	Location	Privilege
Trial License Control	Block free trial sign-ups without admin permission	Azure PowerShell	Azure PowerShell Admin
Control agents with AI Features	Block generative AI usage in Copilot agents	PPAC → Settings	Power Platform Admin
Copilot Studio Authors Control	Restrict Copilot Studio usage to a security group	PPAC → Settings	Power Platform Admin

Setting	Purpose	Location	Privilege
Set Up Environment Routing	Route makers to specific environment groups	PPAC → Settings	Power Platform Admin
AI Builder Credits Control	Decide if tenant-level AI credits can be used by envs	PPAC → Settings	Power Platform Admin
Copilot Data Collection	Enable or block sharing prompts/requests with Microsoft	PPAC → Settings	Power Platform Admin
Copilot Feedback Control	Enable or block feedback to Microsoft	PPAC → Settings	Power Platform Admin

Tenant or Environment-Level (via DLP Policies or Capacity)

Setting [Name]	Purpose	Location	Privilege
Message Capacity	Allocate Copilot message capacity to each environment	PPAC → Capacity	Power Platform Admin
Telemetry Logging / AppInsights Control *[Application insights in Copilot Studio]*	Block agent makers from connecting to Application Insights	PPAC → DLP Policies	Power Platform Admin
Authentication Control *[Chat without Microsoft Entra ID authentication in Copilot]*	Disable “No-Auth” & “Generic OAuth” as Copilot auth providers	PPAC → DLP Policies	Power Platform Admin
Channel Control	Block channels (Direct Line,	PPAC → DLP Policies	Power Platform Admin

Setting [Name]	**Purpose**	**Location**	**Privilege**
[Microsoft Teams + M265 Channel in Copilot Studio] *[Direct Line Channels in Copilot Studio]* *[Facebook Channel in Copilot Studio]* *[Omni Channel in Copilot Studio]*	Facebook, M365, Teams, OmniChannel)		
Knowledge Source Control *[Knowledge source with SharePoint and OneDrive in Copilot Studio]* *[Knowledge source with Public website and data in Copilot Studio]* *[Knowledge source with documents in Copilot Studio]*	Block SharePoint, OneDrive, Documents, or public websites to be used as a knowledge source in agents.	PPAC → DLP Policies	Power Platform Admin
Skills Control *[Skills with Copilot Studio]*	Block Copilot makers from using Skills in Copilot Studio	PPAC → DLP Policies	Power Platform Admin
HTTP Requests Control *[HTTP]*	Prevent HTTP requests to reduce data exfiltration risk	PPAC → DLP Policies	Power Platform Admin
Event Triggers Control (Autonomous) [Microsoft Copilot Studio]	Block autonomous/event-driven agent triggers	PPAC → DLP Policies	Power Platform Admin

Environment-Level Settings

Setting	Purpose	Location	Privilege
Generative AI Control (Bing Search)	Allow or block Bing Search in Copilot agents	PPAC → Environment → Generative AI Features	Environment Admin
AI Prompts Control	Enable or block AI prompts in Power Platform	PPAC → Environment → Features	Environment Admin
Copilot in Power Apps	Enable or block Copilot in Power Apps	PPAC → Environment → Features	Environment Admin
Block Solutions w/ Unmanaged Custom.	Prevent importing unmanaged customizations	PPAC → Environment → Features	Environment Admin
Sharing Agents (Editor/Viewer)	Manage if agents can be shared w/ Editor/Viewer roles	PPAC → Environment Groups (Managed Env)	Environment Admin
Environment Auditing	Enable auditing in production environments	PPAC → Environment Settings → Auditing	Environment Admin
Maker Welcome Message	Display privacy/compliance message to makers	PPAC → Environment Groups (Managed Environment)	Power Platform Admin

Agent-Level Settings (Within Copilot Studio)

Setting	Purpose	Location	Privilege
Agent Authentication	Configure (No Auth, Entra ID, Certificates)	Copilot Studio → Your Agent → Settings → Security → Auth	Agent Author
Agent Web Channel Security	Manage secrets/tokens for Direct Line web channel	Copilot Studio → Your Agent → Settings → Security → Auth	Agent Author

Copyright