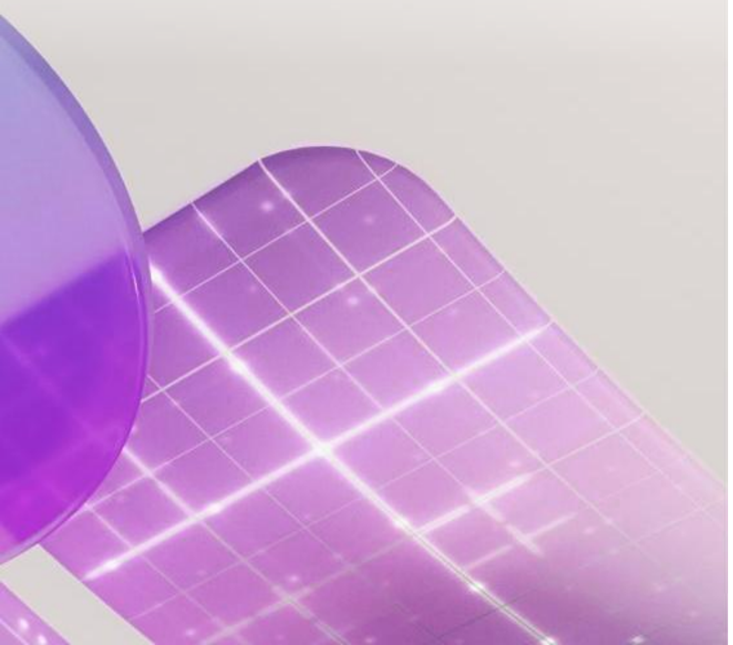
Microsoft

The CIO Playbook to Governing AI Agents in a Low-Code World

Extending Power Platform Governance into the Age of AI

Start →

Table of contents



The CIO playbook to Governing AI Agents in a Low-Code World

This guide is intended for organizations that have established familiarity with Power Platform technologies and governance. It outlines strategies to expedite the adoption of Copilot Studio and agents by leveraging your existing foundations.

AI Agent: Specialized AI systems designed to perform tasks, make decisions and interact with systems either under direction or autonomously.

Low code: A software development approach that enables both professional developers and non-developers to build applications, automate workflows, and create AI agents using visual tools, drag-and-drop interfaces, and AI-assisted authoring—with minimal or no coding required.

Introduction

Introduction

AI agents are poised to become ubiquitous in the enterprise—augmenting decisions, automating tasks, and unlocking new efficiencies. But with this power comes great responsibility. CIOs who lead with foresight and structure will be the ones who turn AI agents into a competitive advantage, not a compliance risk.

According to Microsoft's 2025 Work Trend Index, Frontier Firms—organizations powered by intelligence on tap and human-agent teams—are emerging through three phases of AI evolution, from assistants to autonomous agents, redefining collaboration as humans shift from users to orchestrators of digital labor.

With CIOs increasingly accountable for AI and agent strategies, governance plays a critical role in scaling agents effectively. The challenge is no longer just about enabling agents but about governing it at scale—ensuring agents are secure, compliant, cost-effective, and aligned with business goals. That also means embedding Responsible AI principles—like fairness, transparency, and accountability—into the way agents are designed, deployed, and monitored.

For years, Microsoft Power Platform has empowered organizations to scale low-code apps and automation with the right governance, controls, and operational models in place. That foundation now extends to AI agents. Since Microsoft Copilot Studio is built on the developments, learnings and successes of the Power Platform, organizations can move even faster reusing and extending their existing investments. In fact, Microsoft itself has been through this evolution. Read the full story on Microsoft's approach here.

Change the way you work with agents

Agility

Modernize automation

Optimize existing business processes with agents that can improve legacy technology

Efficiency

Innovate with new processes

Unlock untapped business value by connecting across data silos to automate new problems

Scalability

Empower everyone with agents

Enable end users in every function and department to address their individual business problems

Introduction

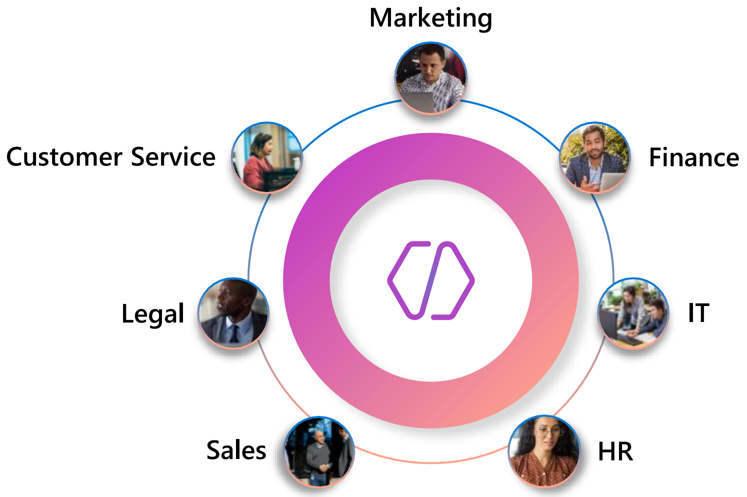
Copilot Studio plays a leading role in the AI agent shift. According to Microsoft's FY25 Q3 earnings release, Copilot Studio has been used by over 230,000 organizations, including 90% of the Fortune 500[1]. IDC project 1.3 billion AI agents by 2028[2]. The scale and speed of adoption make one thing clear: governance is emerging as a critical priority.

This eBook outlines five strategic pillars for governing AI agents. Together, they form the foundation of an operational model built from the success of Power Platforms low code approach, enabling innovation at scale while maintaining control. Each pillar represents a core function of the CoE, from policy and oversight to enablement and culture.

Whether you're just beginning your agent journey or scaling across the enterprise, this guide will help you understand that your low code governance models can be reused and extended to empower your teams with the latest agent technology and innovation —without compromising trust, security, or accountability.

This guide outlines a strategic roadmap across five key pillars

1. A Governance Mindset Is Essential for Agents
2. Low-code Lessons Apply Directly to Agents
3. Driving Visibility, Cost Control, and Business Value
4. Empower Innovation with Guardrails
5. Community, Training, and Experimentation Drive Adoption

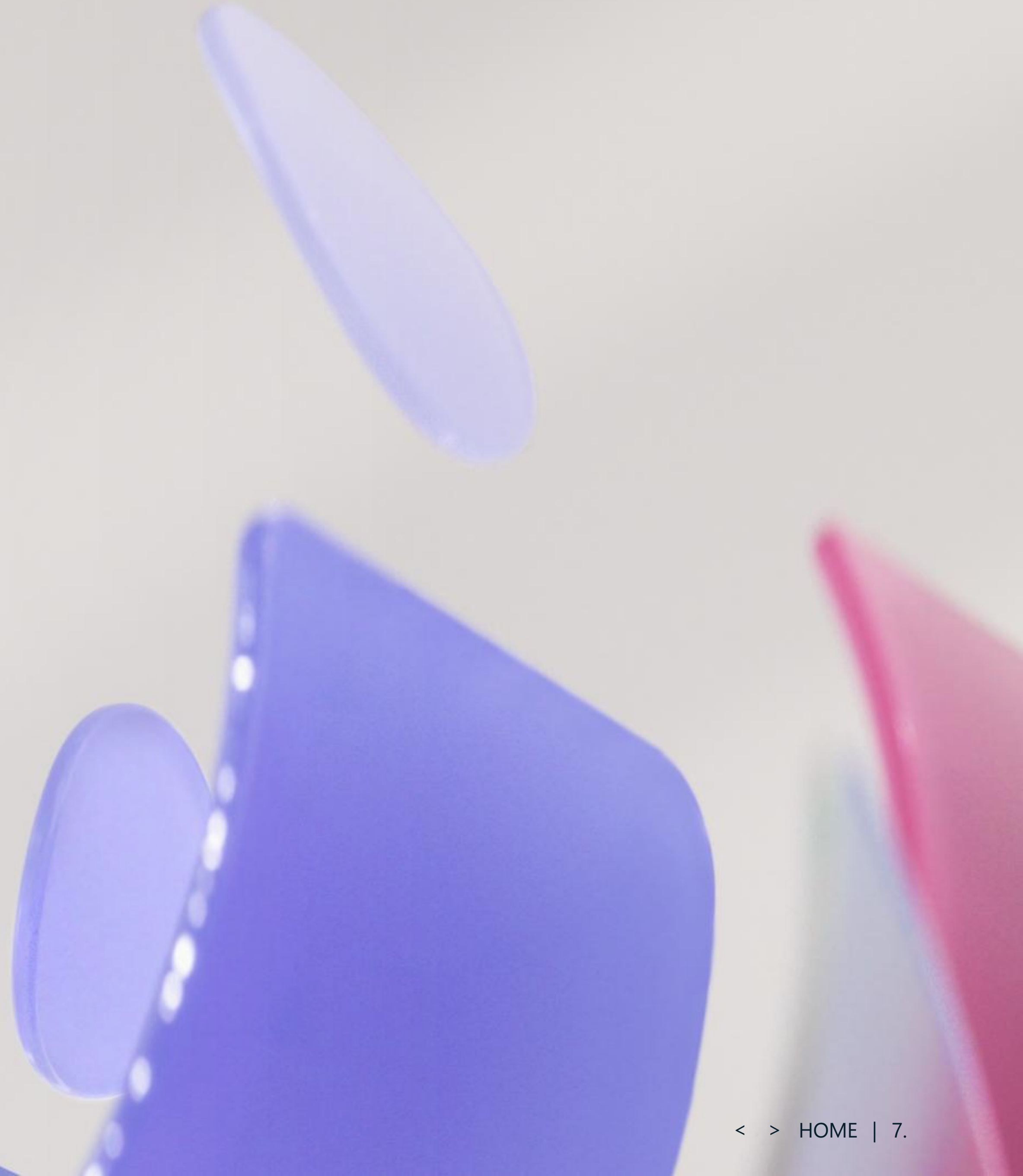


IDC project **1.3 billion AI agents** by 2028[2]

[1]: Microsoft Earnings Release, Call Transcript, FY25, Q3
[2]: IDC Info Snapshot, sponsored by Microsoft, 1.3 Billion AI Agents by 2028, #US53361825 and May 2025

SECTION ONE

A Governance Mindset Is Essential for Agents



Understanding the Agent Shift

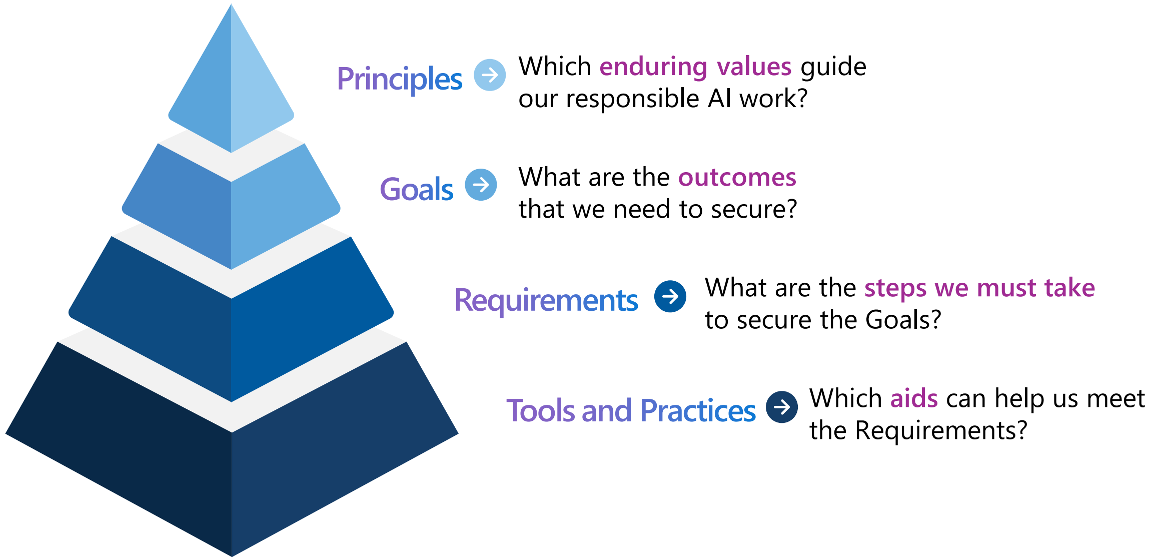
AI agents aren't just another IT capability—they represent a fundamental shift in how work gets done. As these systems evolve from passive assistants to autonomous actors, CIOs must lead with a governance mindset that aligns agents with enterprise strategy, risk posture, and cultural values.

But governance doesn't start in a vacuum. It follows vision. CIOs must first define how agents will drive business value—where they'll have the biggest impact, how success will be measured, and who needs to be involved. That vision should guide a broader adoption strategy. This playbook assumes that foundation and vision is already in place. If not, use the agent adoption resources for IT leaders here.

Once the vision is clear, governance becomes the enabler. It ensures agents are secure, compliant, cost-effective, and aligned with business goals. This is more than a technical challenge—it's a leadership opportunity. CIOs are uniquely positioned to define how agents are introduced, governed, and scaled. That starts with executive alignment: governance must be tied to business outcomes, not just compliance.

Responsible AI must be embedded into the organization's operating model. It's not just about avoiding harm—it's about building trust, managing risk, and ensuring AI and agents reflects your company's values. Define what AI means in your organization, and make that definition actionable through policy, oversight, and accountability. Learn more about Responsible AI at Microsoft here. Make use of Responsible AI tools such as the AI impact assessment guide and Human-Experience experience toolkit.

The anatomy of responsible AI



Principles → Which **enduring values** guide our responsible AI work?

Goals → What are the **outcomes** that we need to secure?

Requirements → What are the **steps we must take** to secure the Goals?

Tools and Practices → Which **aids** can help us meet the Requirements?

The rise of the Frontier firm

As mentioned in Microsoft's Work Trend Index, organizations are seeing a three phased approach in adopting the news ways of work with agents. CIOs should assess agent maturity in the workplace and adjust oversight as solutions become more advanced and widely adopted.

Phase 1: Human with Assistant

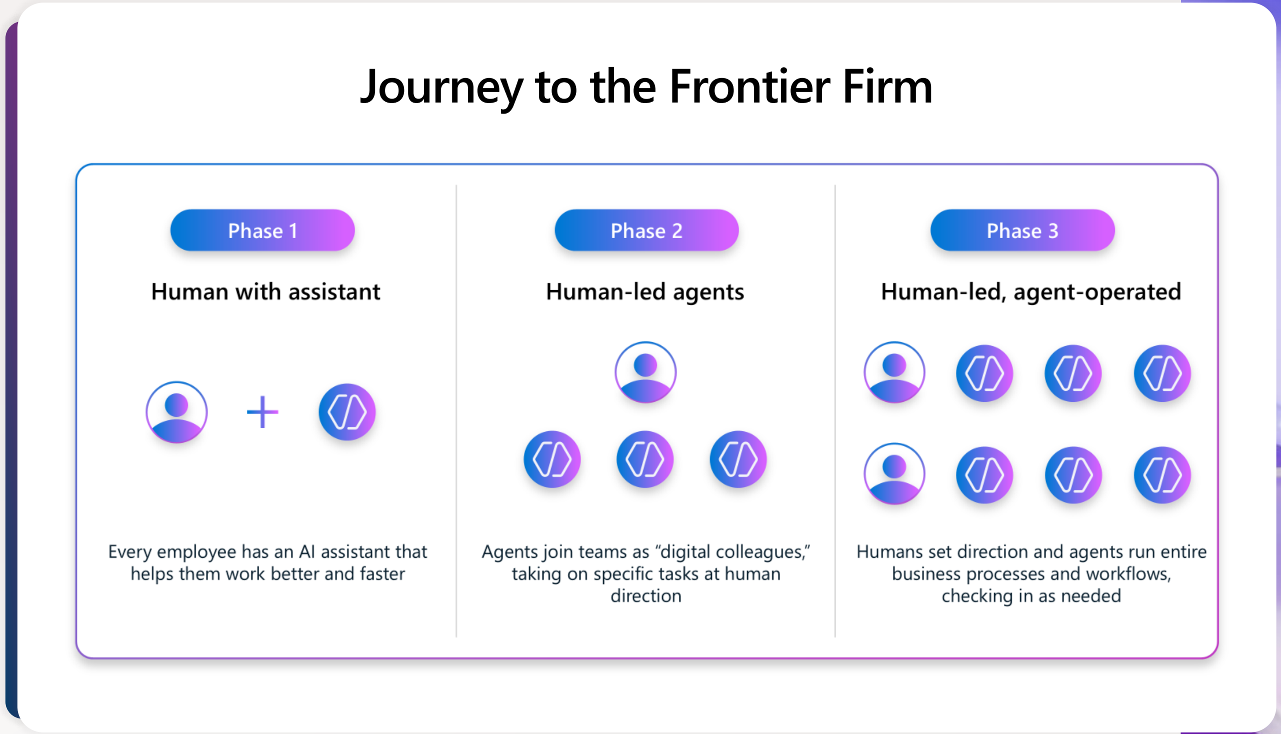
AI agents begin as personal assistants—automating repetitive tasks, summarizing content, and surfacing insights. This phase is about augmenting individual productivity without fundamentally changing workflows.

Phase 2: Human-Agent Teams

Agents evolve into digital colleagues embedded in teams. They take on specific tasks with human direction—drafting proposals, analyzing data, managing workflows. This introduces new dynamics in collaboration and accountability. CIOs must define how agents are integrated into team structures, how their outputs are validated and compliant, and how performance is measured.

Phase 3: Human-Led, Agent-Operated

Agents become autonomous operators of business processes, with humans setting direction and stepping in only when needed. This redefines the nature of work and demands adaptive oversight.



Journey to the Frontier Firm

Phase 1

Human with assistant

Every employee has an AI assistant that helps them work better and faster

Phase 2

Human-led agents

Agents join teams as "digital colleagues," taking on specific tasks at human direction

Phase 3

Human-led, agent-operated

Humans set direction and agents run entire business processes and workflows, checking in as needed

Meet the Agent Boss

The human-agent interaction is developing. IT oversees agents across the organization, while employees are increasingly managing agents day to day themselves, calling for new working methods, cultural adjustments, and require targeted training.

Just like effective people managers, agent managers develop teams with intentionality, and delegate responsibilities judiciously. Designing agents with well-defined roles tailored to specific business needs is crucial; it is advisable to begin with straightforward objectives and maintain precision in execution.

It is important to **calibrate the ratio of human oversight to agent autonomy**, as greater independence may necessitate enhanced monitoring processes. Optimizing agent performance requires continuously refining instructions and systematically evaluating their impact, including return on investment (ROI).

We're no longer just using AI tools—we're leading them. The best agent bosses think like managers: building teams strategically, managing them with clear communications, and delegating wisely.

You can learn more about how to be an agent boss here.

Building agents

Create agents with a clear job description that solves a real business problem. Start simple. Be specific.

Delegating to agents

Think about your human-agent ratio. You'll likely need more human oversight when agents have greater autonomy vs responding to prompts.

Managing agents

Improve underperforming agents by refining their instructions over time. Do performance reviews—yes, even for agents. Measure the ROI and impact.

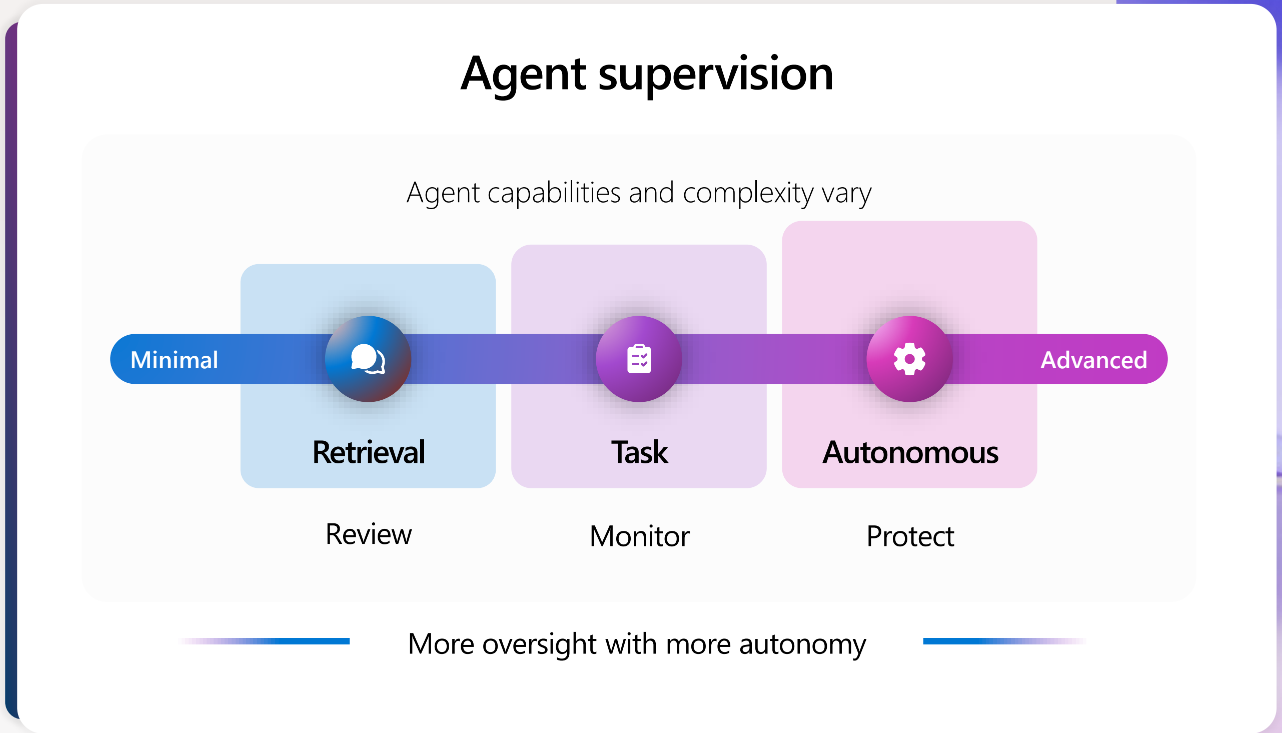
Adaptive Oversight for Agent Autonomy

Agents differ from traditional software in one critical way: they don't just suggest actions—they take them. This shift demands an evolving model of oversight. CIOs must define how much autonomy agents are granted, how they're integrated into teams, and how their actions stay aligned with business goals.

Governance must evolve from static controls to adaptive oversight. Policies can't be "set and forget"—they need to be monitored, updated, and enforced continuously for the new way of work. CIOs should treat agents like digital labor: they require identity management, lifecycle tracking, and access controls. Not all agents need the same level of freedom.

Define levels of autonomy based on risk and context

- **Reviewers** verify AI-generated output for accuracy and appropriate use.
- **Monitors** track agent actions and enable human or AI-based follow-up.
- **Protectors** can adjust or restrict agent permissions in real time using automated controls.



Agent supervision

Agent capabilities and complexity vary

Minimal → Advanced

Retrieval	Task	Autonomous
Review	Monitor	Protect

More oversight with more autonomy

Balancing Innovation through Governance

Autonomy introduces new risks—data leaks, policy breaches, model drift—but **these are manageable with the right governance in place**. CIOs can scale agent adoption confidently by applying proven controls, continuous monitoring, and responsible AI practices.

Set clear boundaries for agent use. Leverage data loss prevention policies, environment strategies using the Power Platform Admin Center, and Microsoft Purview to ensure agent actions are visible and auditable. The next section provides more detail.

Empower agent creators to build and deploy their own solutions unlocks speed, creativity, and scale—but it also introduces new responsibilities. **Striking the right balance between autonomy and oversight ensures that innovation** can thrive without compromising security, compliance, or operational integrity.

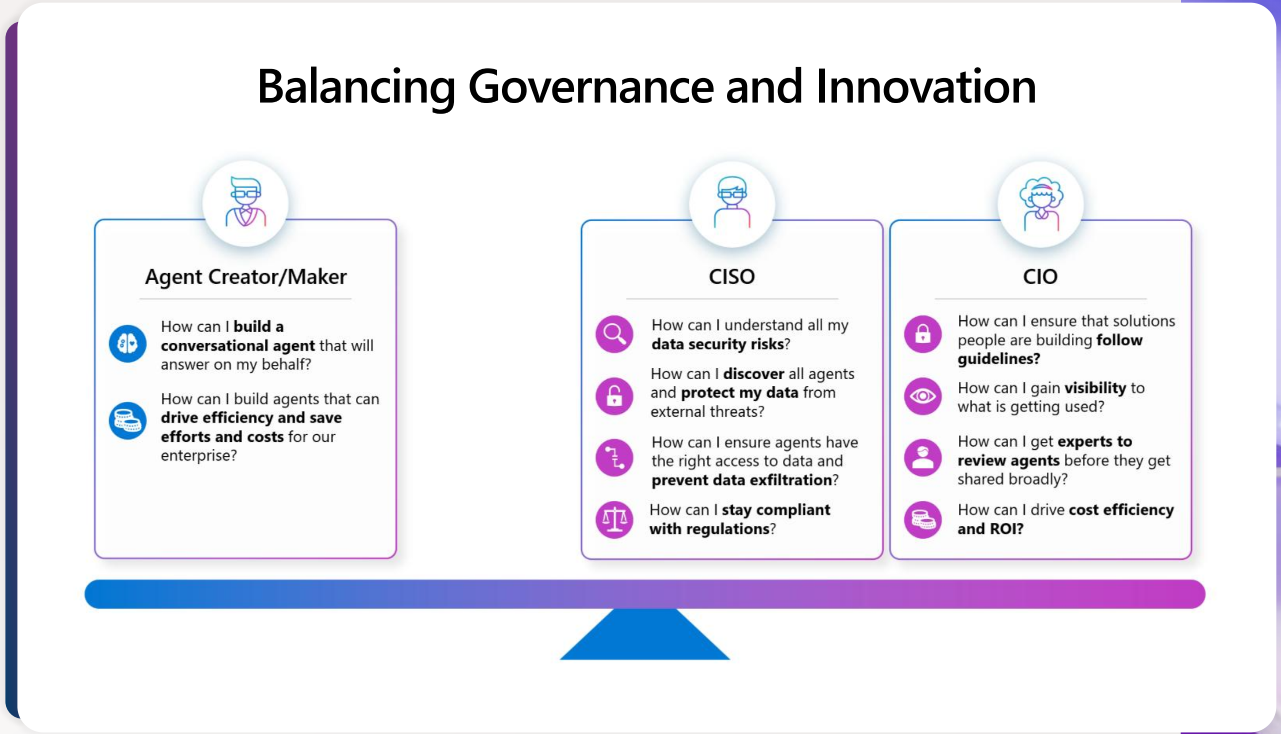
From Static Controls to Adaptive Oversight

Traditional Apps

- Static logic
- User-initiated
- Fixed rules
- Manual oversight
- Role-based access

AI Agents

- Dynamic behavior
- User or Agent-initiated
- Evolving policies
- Continuous monitoring
- Risk-based autonomy



Balancing Governance and Innovation

Agent Creator/Maker

How can I **build a conversational agent** that will answer on my behalf?

How can I build agents that can **drive efficiency and save efforts and costs** for our enterprise?

CISO

How can I understand all my **data security risks**?

How can I **discover** all agents and **protect my data** from external threats?

How can I ensure agents have the right access to data and **prevent data exfiltration**?

How can I **stay compliant with regulations**?

CIO

How can I ensure that solutions people are building **follow guidelines?**

How can I gain **visibility** to what is getting used?

How can I get **experts to review agents** before they get shared broadly?

How can I drive **cost efficiency and ROI?**

An Operational Model to Thrive

It isn't just about tools—it's about rhythms, roles, and responsibilities. A well-structured operating model ensures innovation and oversight move in lockstep.

AI leadership sets the vision and makes strategic investment decisions.

Senior leadership aligns AI priorities with business needs and navigates build-vs-buy decisions.

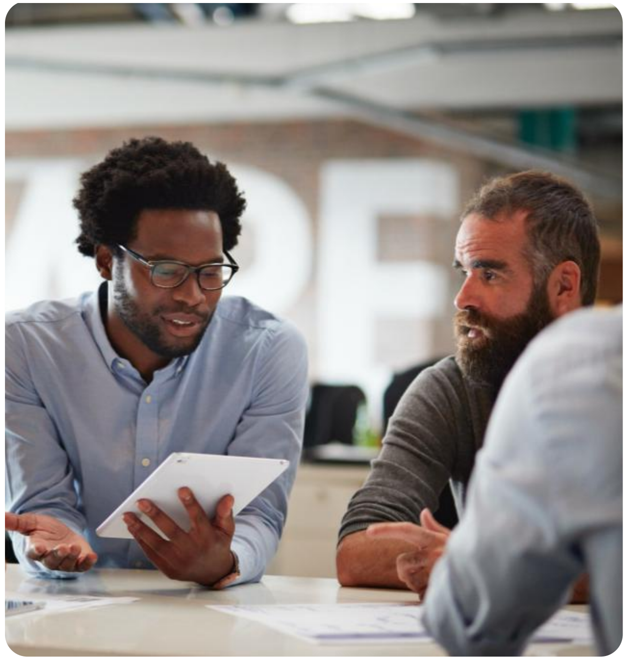
Governance teams maintain standards, safety, and scalability through weekly oversight.

Citizen developers and IT teams drive day-to-day execution, adoption, and skill-building.

This structure is designed to support a balance of innovation, oversight, and continuous improvement. Section 3 offers a deep dive into this approach.

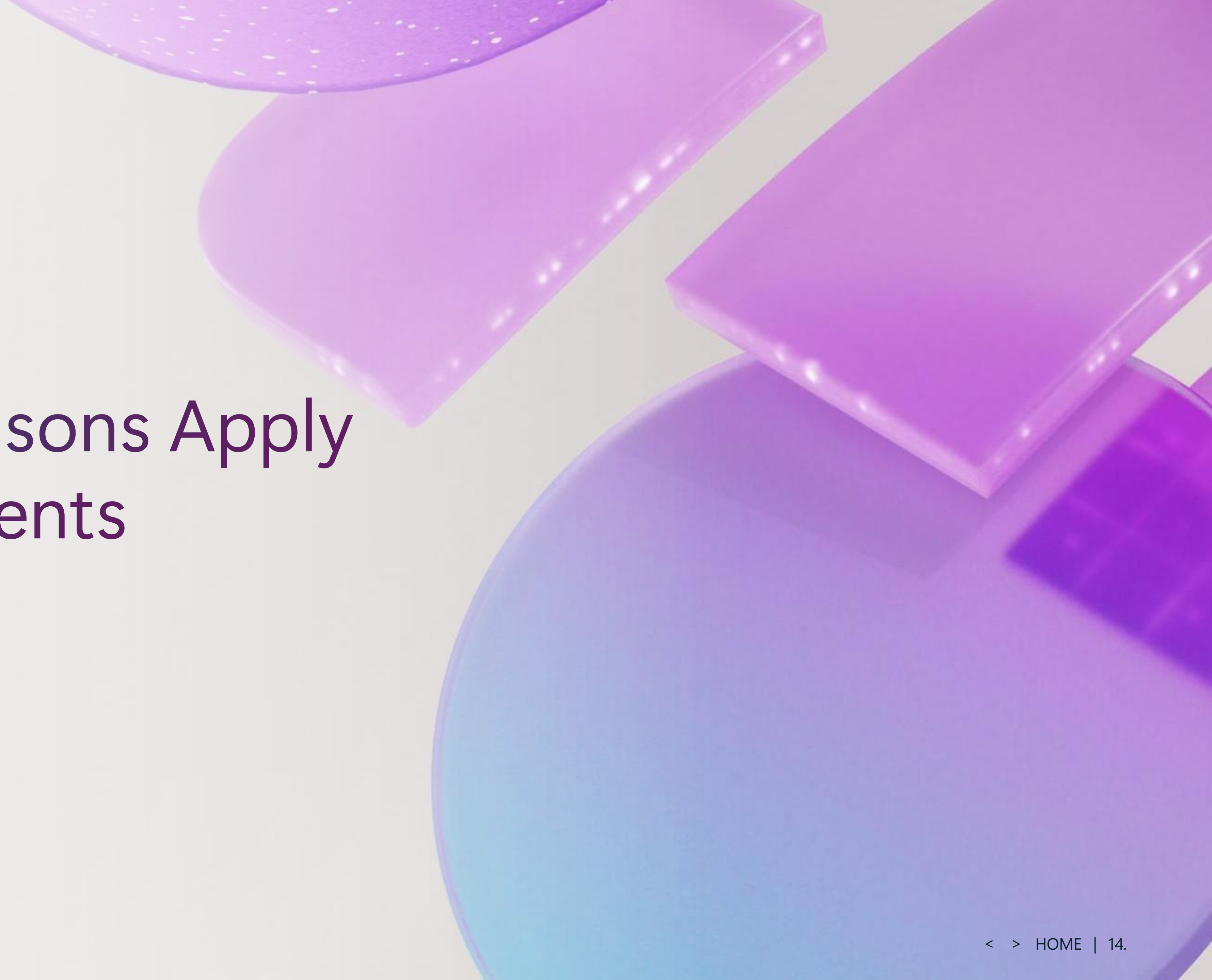
CIO Checklist

- ❑ Define what responsible AI means in your organization (CIO / Chief Ethics Officer)
- ❑ Treat agents as digital colleagues with identity, access, and lifecycle controls (IT Security / IAM Lead)
- ❑ Establish levels of agent autonomy based on risk and use case (CoE Lead / Risk Officer)
- ❑ Shift from static policies to adaptive oversight with continuous monitoring (CISO / Compliance Officer)
- ❑ Ensure agent actions are visible and auditable (IT Ops / Security Admin)



SECTION TWO

Low-Code Lessons Apply Directly to Agents



Low-Code Lessons Apply Directly to Agents

The good news is that you don’t need to start from scratch. To manage agents at scale, CIOs should think in terms of four strategic pillars:

Security, Governance, Operations, and Availability. These pillars mirror the Power Platform governance model and apply directly to Copilot Studio. For example, Centers of Excellence (CoEs), environment strategies, and connector management policies—are not just relevant to AI agents, they’re essential. These proven models form the backbone of a modern AI governance strategy.

A fully managed platform to enable, scale, and reduce risk

CISO	CIO	Head of Operations	Head of Operations
MANAGED SECURITY	**MANAGED GOVERNANCE**	**MANAGED OPERATIONS**	**MANAGED AVAILABILITY**
Advanced protection for an AI-driven world	**More visibility, More Control, Less effort**	**Operational excellence for agents at scale**	**Enterprise Grade Reliability and Availability for Mission Critical Workloads**
Security posture management	Management at scale	App lifecycle management	Hyper Availability (Az)
Threat protection	Environment strategy	Observability	BCDR Agility
Data protection and privacy	Reactive governance	Data Retention and Mobility	
Identity and access management	Full visibility	Quality checker	
Compliance	Capacity and cost management	Test automation	

Low-Code Lessons Apply Directly to Agents

1. Security: Protecting Data and Access

Start by extending your existing security posture for apps and automation to agents. Use identities and access controls to manage who can create, deploy, and run agents. Apply DLP policies to control what data agents can access or share. Sensitivity labels, data classification, and access reviews help maintain a unified security model across apps, flows, and agents. Copilot Studio also supports geographic data residency and customer-managed encryption keys (CMK) to meet regulatory requirements. Learn more and review the security check list.

2. Governance: Policy, Oversight, and Lifecycle

Governance is about more than control—it's about enabling safe innovation, and not outpacing accountability. Many organizations are **evolving their Power Platform CoEs into AI CoEs**, expanding their scope to include agent standards, training, and oversight. Microsoft Digital, for example, built on its existing low-code governance to review internally created agents with the same rigor as enterprise apps. Power Platform's Managed Environments provide a scalable way to group agents, apply policies, and gain visibility into maker activity.

Copilot Studio provides essential agent control features, such as tenant-level controls to block or allow custom agents, restrict publishing channels, and present maker banners for privacy and compliance reminders. Ongoing feedback among makers, admins, and the CoE helps ensure these guardrails remain effective yet adaptable. Learn more

3. Operations: Deployment and monitoring

Operational rigor is essential to scaling agents safely. Extend your existing Application Lifecycle Management (ALM) practices to agents—moving them through development, testing, and production stages using Power Platform pipelines and DevOps tooling. This ensures agents are version-controlled, tested, and production-ready.

Copilot Studio also provides operational visibility. Each key action—from creation to publishing—can be logged and auditable. Integrated with Microsoft Purview and Sentinel, these logs enable real-time monitoring, anomaly detection, and proactive security response. Together, these capabilities give CIOs the confidence to scale agent operations with control and clarity. Learn more

4. Availability: Business Continuity for Critical Workloads

In today's enterprise, downtime isn't just inconvenient—it's costly. Traditional backup and restore methods are too slow for modern demands. **Organizations now require immediate failover, automated resilience, and uninterrupted operations.**

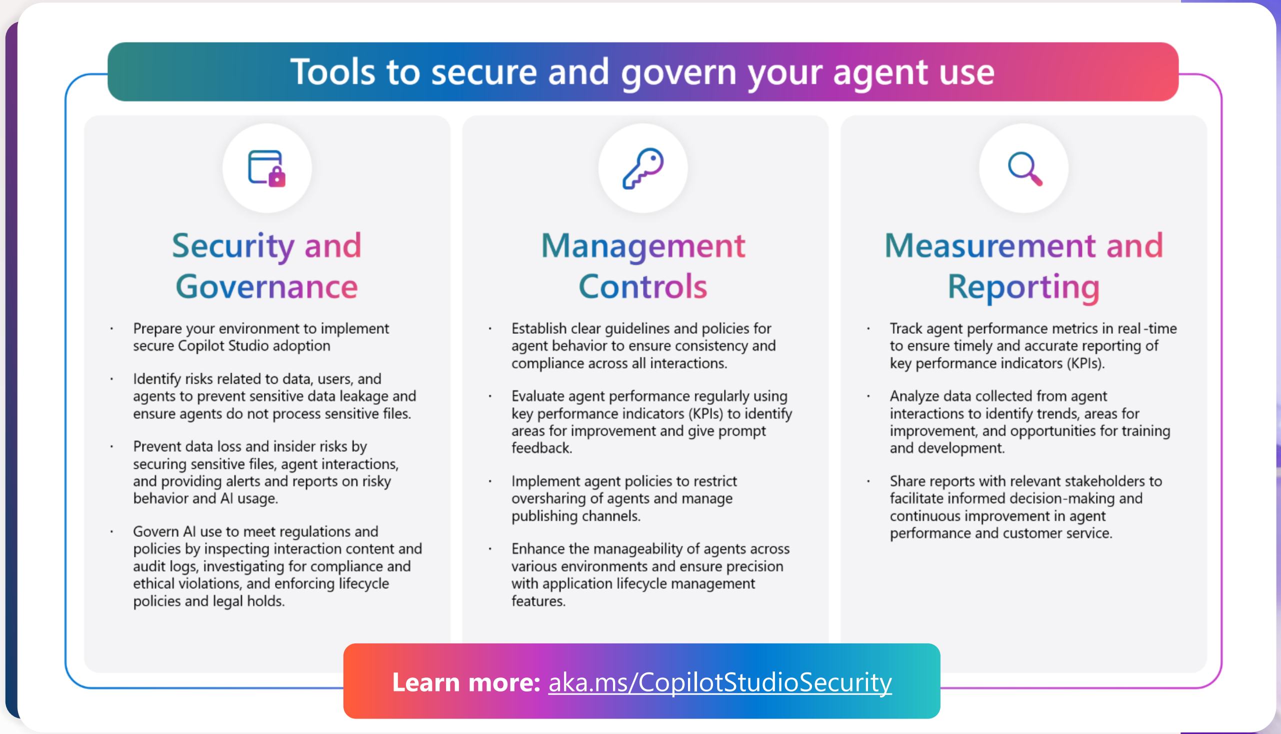
Managed Availability is a set of capabilities designed to support these mission-critical applications and AI workloads.

It leverages Azure Availability Zones to ensure near-zero downtime and minimize service interruptions. IT teams can initiate cross-region disaster recovery on their own—no support ticket required—enabling faster, more flexible failover. Automated backups with point-in-time restore capabilities protect data integrity and support operational continuity. And with self-serve disaster recovery drills, teams can validate readiness and meet compliance and audit requirements without disrupting production. Learn more

Low-Code Lessons Apply Directly to Agents

By organizing your governance strategy around these pillars, you can scale agent adoption with confidence—reusing familiar tools, reducing friction, and accelerating time to value. For CIOs, this continuity is more than operational efficiency—it's a strategic advantage.

Governance Area	How It Applies to AI Agents
Identity & Access	Use Entra ID and RBAC to manage who can create, deploy, and run agents
Environment Strategy	Develop an environment strategy to isolate dev/test/prod agent workspaces
Data Loss Prevention	Extend DLP policies to control what data agents can access or share
Auditing & Monitoring	Use Microsoft Purview and Defender to track agent behavior and flag anomalies
Compliance & Risk	Apply existing compliance frameworks to ensure agents meet regulatory and internal standards
CoE & Governance Teams	Expand existing low-code CoEs to include agent development and oversight



Tools to secure and govern your agent use

Security and Governance

- Prepare your environment to implement secure Copilot Studio adoption
- Identify risks related to data, users, and agents to prevent sensitive data leakage and ensure agents do not process sensitive files.
- Prevent data loss and insider risks by securing sensitive files, agent interactions, and providing alerts and reports on risky behavior and AI usage.
- Govern AI use to meet regulations and policies by inspecting interaction content and audit logs, investigating for compliance and ethical violations, and enforcing lifecycle policies and legal holds.

Management Controls

- Establish clear guidelines and policies for agent behavior to ensure consistency and compliance across all interactions.
- Evaluate agent performance regularly using key performance indicators (KPIs) to identify areas for improvement and give prompt feedback.
- Implement agent policies to restrict oversharing of agents and manage publishing channels.
- Enhance the manageability of agents across various environments and ensure precision with application lifecycle management features.

Measurement and Reporting

- Track agent performance metrics in real -time to ensure timely and accurate reporting of key performance indicators (KPIs).
- Analyze data collected from agent interactions to identify trends, areas for improvement, and opportunities for training and development.
- Share reports with relevant stakeholders to facilitate informed decision-making and continuous improvement in agent performance and customer service.

Learn more: aka.ms/CopilotStudioSecurity

You can review the security overview and strategy content here for additional information: Security overview and strategy

CIO Checklist

- ❑ Extend existing low-code governance structures to include AI agents (CIO / CoE Lead)
- ❑ Apply DLP, environment strategies, and connector policies to agent development (IT Admin / Security Admin)
- ❑ Implement ALM practices for agent lifecycle management (DevOps Lead / Platform Admin)
- ❑ Expand the CoE to include agent standards and oversight (CoE Lead / CIO)
- ❑ Monitor agent usage and compliance through unified admin tools (IT Ops / Compliance Officer)

SECTION THREE

Driving Visibility, Cost Control, and Business Value

Driving Visibility, Cost Control, and Business Value

CIOs need a clear line of sight into how agents are created, used, and scaled. Visibility, telemetry, and cost control are crucial to ensure that agent adoption doesn't overtake governance.

As agents proliferate, **centralized visibility becomes non-negotiable**. Without it, agents can sprawl across departments—leading to redundancy, inconsistent quality, and security blind spots.

CIOs need to know

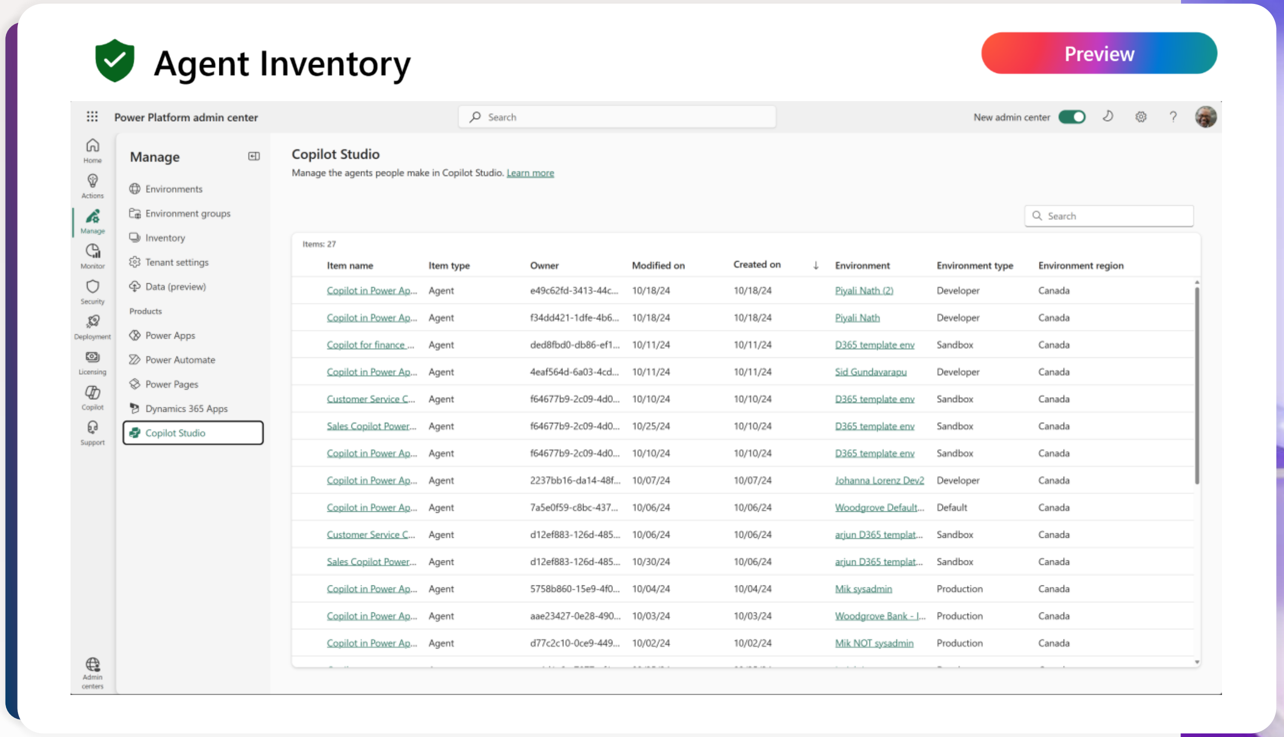
- What agents exist?
- Who built them?
- What data do they access?
- How much do they cost?
- What's the business value they bring?

Track, Monitor, and Manage at Scale

Track agents across your organization—including makers, usage patterns, and access permission using dashboards in the Power Platform Admin Center and Entra Agent ID (Preview). This inventory helps identify high-impact agents worth scaling and low-value or risky ones to retire.

Publishing an agent, configuring connectors, and modifying access are logged as part of Copilot Studio's audit trail. These logs integrate with Microsoft Purview, giving IT teams end-to-end visibility and traceability across the agent lifecycle—from creation to deployment and usage.

You can monitor agent performance and behavior using the out of the box analytics in Copilot Studio and the Power Platform Admin Center, with more advanced monitoring using Azure Monitor Insights. These tools provide deep telemetry, anomaly detection, and security monitoring.



Agent Inventory

Preview

Copilot Studio

Manage the agents people make in Copilot Studio. Learn more

Items: 27

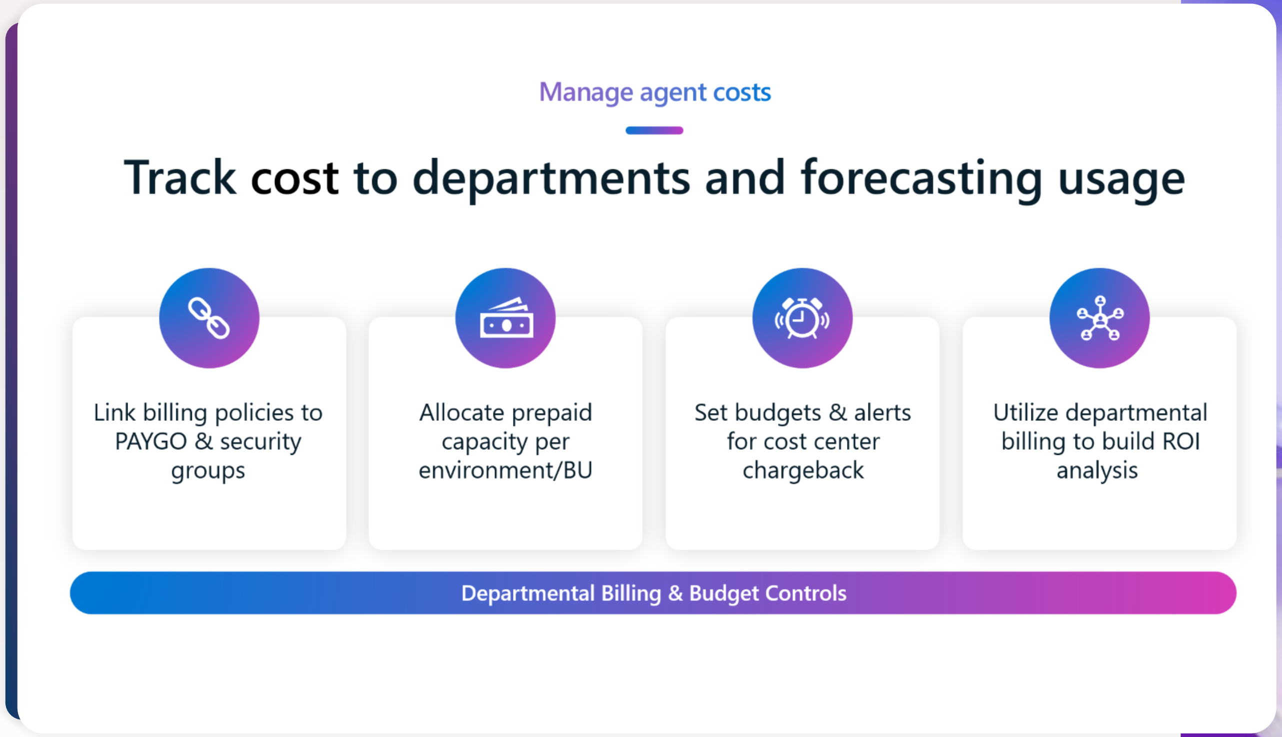
Item name	Item type	Owner	Modified on	Created on ↓	Environment	Environment type	Environment region
Copilot in Power Ap...	Agent	e49c62fd-3413-44c...	10/18/24	10/18/24	Piyali Nath (2)	Developer	Canada
Copilot in Power Ap...	Agent	f34dd421-1dfe-4b6...	10/18/24	10/18/24	Piyali Nath	Developer	Canada
Copilot for finance ...	Agent	ded8fbd0-db86-ef1...	10/11/24	10/11/24	D365 template env	Sandbox	Canada
Copilot in Power Ap...	Agent	4eaf564d-6a03-4cd...	10/11/24	10/11/24	Sid Gundavarapu	Developer	Canada
Customer Service C...	Agent	f64677b9-2c09-4d0...	10/10/24	10/10/24	D365 template env	Sandbox	Canada
Sales Copilot Power...	Agent	f64677b9-2c09-4d0...	10/25/24	10/10/24	D365 template env	Sandbox	Canada
Copilot in Power Ap...	Agent	f64677b9-2c09-4d0...	10/10/24	10/10/24	D365 template env	Sandbox	Canada
Copilot in Power Ap...	Agent	2237bb16-da14-48f...	10/07/24	10/07/24	Johanna Lorenz Dev2	Developer	Canada
Copilot in Power Ap...	Agent	7a5e0f59-c8bc-437...	10/06/24	10/06/24	Woodgrove Default...	Default	Canada
Customer Service C...	Agent	d12ef883-126d-485...	10/06/24	10/06/24	arjun D365 templat...	Sandbox	Canada
Sales Copilot Power...	Agent	d12ef883-126d-485...	10/30/24	10/06/24	arjun D365 templat...	Sandbox	Canada
Copilot in Power Ap...	Agent	5758b860-15e9-4f0...	10/04/24	10/04/24	Mik sysadmin	Production	Canada
Copilot in Power Ap...	Agent	aae23427-0e28-490...	10/03/24	10/03/24	Woodgrove Bank - I...	Production	Canada
Copilot in Power Ap...	Agent	d77c2c10-0ce9-449...	10/02/24	10/02/24	Mik NOT sysadmin	Production	Canada

Keeping Agent Costs in Check

Cost Control keeps innovation aligned with value. Unchecked agent usage can lead to budget surprises. CIOs can mitigate this by setting agent usage caps, monitoring message consumption and configuring pay-as-you-go meters and alerts so you only pay for what you use.

Read the agent cost management eBook to learn more.

By tracking agents, their consumption and reviewing performance regularly, teams can identify underused or redundant agents, forecast expenses with tools like the cost calculator, and ensure agents stay aligned with strategic goals.



Manage agent costs

Track cost to departments and forecasting usage

- Link billing policies to PAYGO & security groups
- Allocate prepaid capacity per environment/BU
- Set budgets & alerts for cost center chargeback
- Utilize departmental billing to build ROI analysis

Departmental Billing & Budget Controls

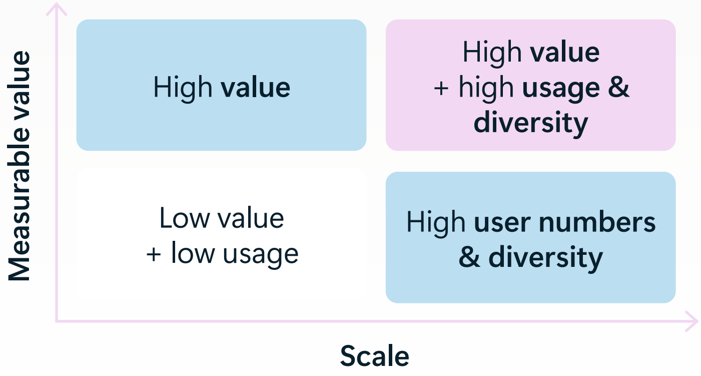
Proving the ROI of Agents

While cost control ensures AI investments don't spiral, **it's business value that ultimately justifies their existence**. CIOs need to go beyond usage caps and budget forecasts to answer a more strategic question: what are agents actually delivering? Business value reframes the conversation from "how much are we spending?" to "what are we getting in return?"

It anchors agent adoption in **intangible gains** like improved employee experience, faster decision-making, and greater agility and **tangible gains** like cost reduced, time saved, or customer satisfaction improved. This shift is critical for aligning agent initiatives with broader business goals and for demonstrating that these tools aren't just novel—they're are becoming increasingly important for organizations seeking to scale AI responsibly.

For CIOs, this means **pairing cost control with a clear value narrative**—one that shows how agents contribute to transformation, not just efficiency. That's what earns executive buy-in and sustains investment.

Learn more how to measure and communicate business value here.



Measurable value

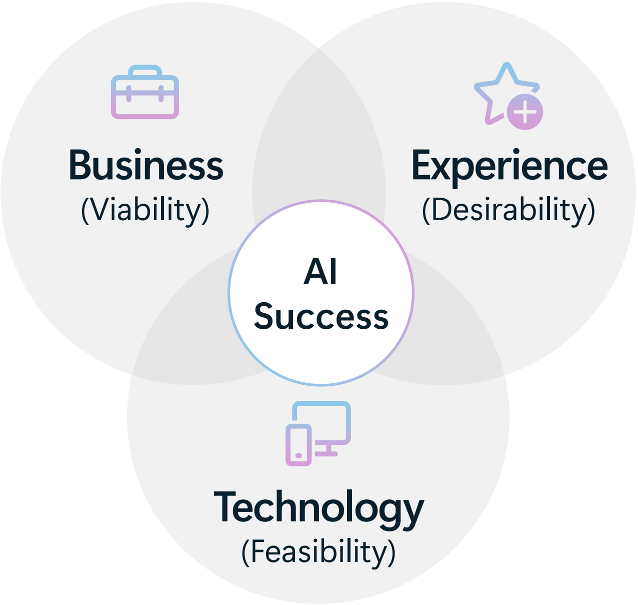
High **value**

High **value**
+ high **usage &**
diversity

Low value
+ low usage

High **user numbers**
& diversity

Scale



Business
(Viability)

Experience
(Desirability)

AI
Success

Technology
(Feasibility)

Tangible Gains

- Cost reduction
- Time savings
- Increased customer satisfaction
- Operational efficiency
- Reduced manual workload
- Faster service delivery

Intangible Gains

- Improved employee experience
- Faster decision-making
- Greater organizational agility
- Enhanced innovation culture
- Stronger cross-functional collaboration
- Increased trust in AI systems

CIO Checklist

With the right tools, CIOs can confidently scale agent adoption while enhancing visibility, governance, and cost control.

❑ Maintain an inventory of all AI agents (IT Ops / Platform Admin)

❑ Track agent usage, access, and ownership across environments (Security Admin / CoE Analyst)

❑ Instrument agents with telemetry for performance and anomaly detection (IT Ops / Observability Lead)

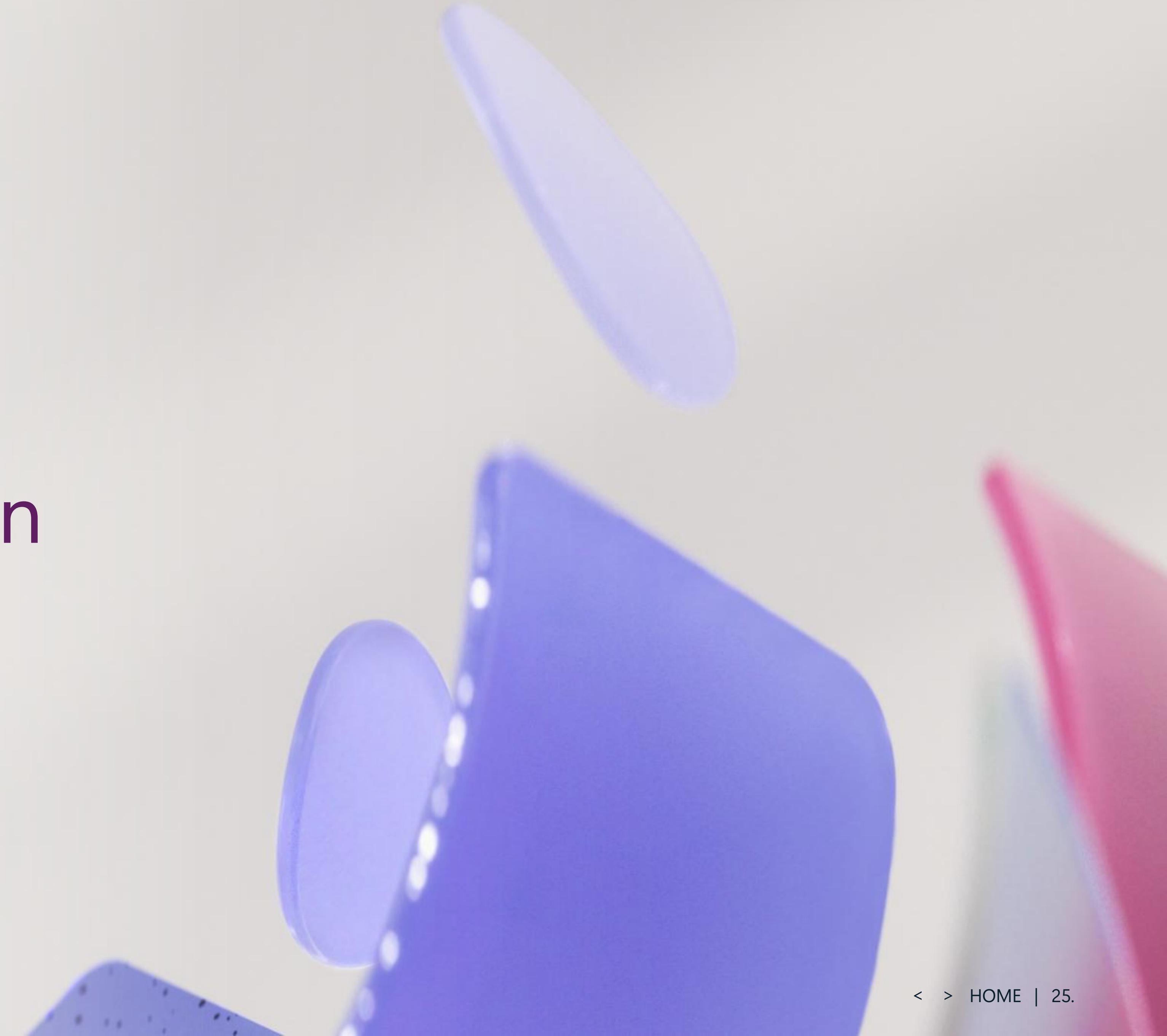
❑ Monitor agent consumption and enforce usage caps (Finance IT / Platform Admin)

❑ Review agent lifecycle to retire unused or redundant agents (CoE Lead / Business Unit IT)

❑ Set up alerts for policy violations or abnormal behavior (Security Operations / CISO)

SECTION FOUR

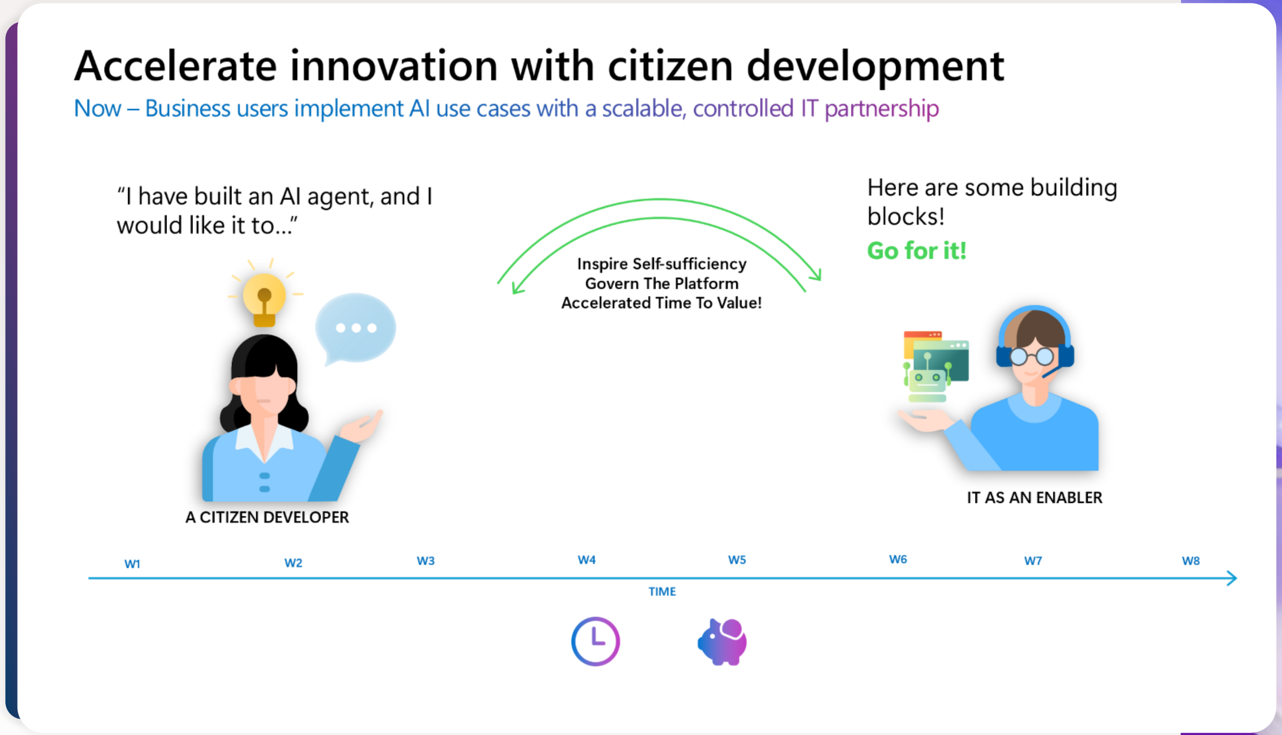
Empower Innovation with Guardrails



Empower Innovation with Guardrails

As organizations move from pilot to scale, **the Center of Excellence (CoE) becomes the engine that enables safe innovation**. It owns the frameworks, tools, and training that allow business users and citizen developers to build confidently—without compromising compliance or control.

Just as the Power Platform empowered employees to build apps and automation, agents now enable them to solve problems with advanced reasoning and orchestration. CIOs must create a secure, governed environment where **experimentation is encouraged**—but always within clear boundaries.



Accelerate innovation with citizen development

Now – Business users implement AI use cases with a scalable, controlled IT partnership

"I have built an AI agent, and I would like to it to..."

Inspire Self-sufficiency
Govern The Platform
Accelerated Time To Value!

Here are some building blocks!
Go for it!

Empower Innovation with Guardrails

To support safe scaling, organizations can adopt **the Zoned Governance Model**—a structured approach that aligns governance maturity with agent complexity and business risk:

Zone 1: Personal Productivity

The entry point for experimentation. This zone provides isolated environments where individuals can safely explore agent capabilities, guided by baseline governance and security policies.

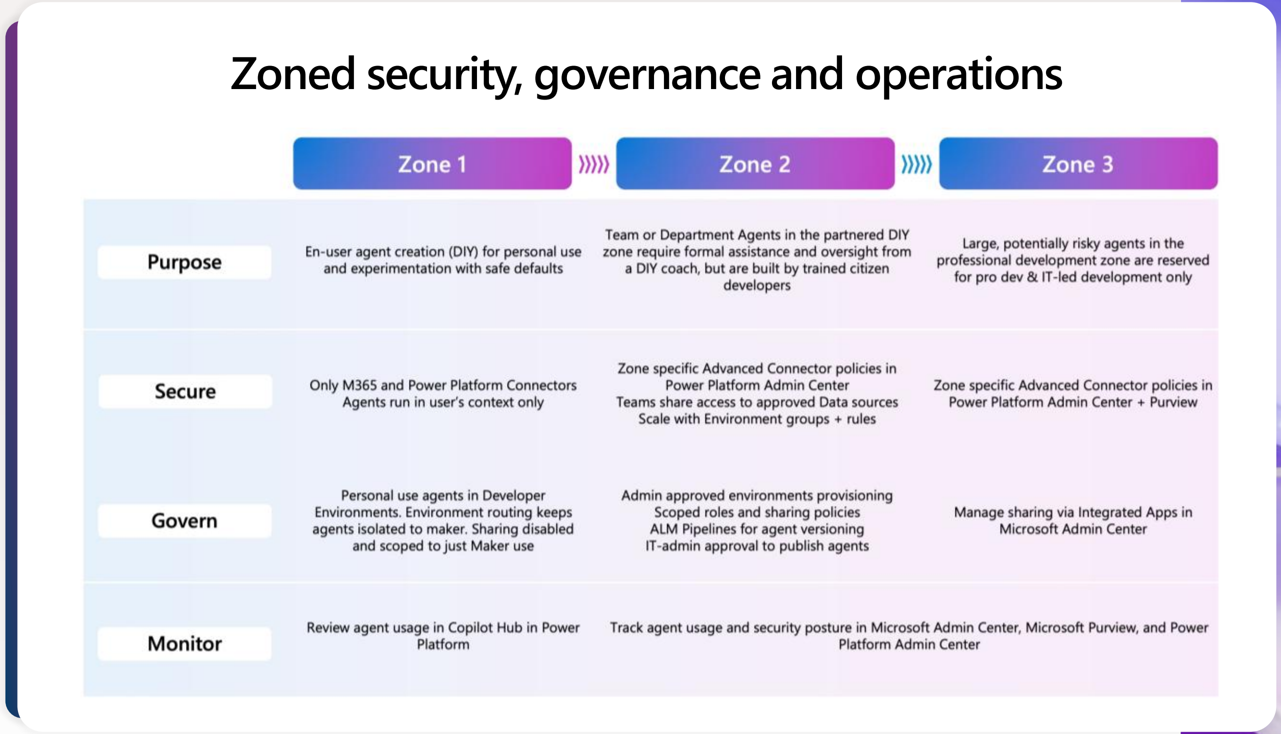
Zone 2: Collaboration

A step up in governance maturity. This zone supports team-based agent development with stronger controls, including environment-level policies, connector restrictions, and operational oversight. It enables broader adoption while maintaining compliance and consistency.

Zone 3: Enterprise Managed

The most advanced zone, designed for production-grade agents. It includes enhanced security protocols (e.g., multi-factor authentication, advanced threat detection), continuous monitoring, and structured lifecycle management. This zone supports complex, cross-functional agent scenarios with full visibility, scalability, and strategic alignment.

This model allows CIOs to match oversight to risk—empowering innovation in lower-risk zones while applying rigorous controls where it matters most. It also gives the CoE a clear framework to guide agent development from experimentation to enterprise deployment.



Zoned security, governance and operations

	Zone 1	Zone 2	Zone 3
Purpose	En-user agent creation (DIY) for personal use and experimentation with safe defaults	Team or Department Agents in the partnered DIY zone require formal assistance and oversight from a DIY coach, but are built by trained citizen developers	Large, potentially risky agents in the professional development zone are reserved for pro dev & IT-led development only
Secure	Only M365 and Power Platform Connectors Agents run in user's context only	Zone specific Advanced Connector policies in Power Platform Admin Center Teams share access to approved Data sources Scale with Environment groups + rules	Zone specific Advanced Connector policies in Power Platform Admin Center + Purview
Govern	Personal use agents in Developer Environments. Environment routing keeps agents isolated to maker. Sharing disabled and scoped to just Maker use	Admin approved environments provisioning Scoped roles and sharing policies ALM Pipelines for agent versioning IT-admin approval to publish agents	Manage sharing via Integrated Apps in Microsoft Admin Center
Monitor	Review agent usage in Copilot Hub in Power Platform	Track agent usage and security posture in Microsoft Admin Center, Microsoft Purview, and Power Platform Admin Center	

Expanding the Center of Excellence (CoE) for the Agent Era

Existing Low Code Centers of Excellence (CoEs) can—and should—expand to include AI agents built in Copilot Studio. But that's just the starting point. As AI adoption accelerates across multiple platforms, **CIOs must ensure their CoE isn't operating in a silo.**

A modern AI CoE should define shared standards, provide training, review agent designs, and **act as a governance bridge between IT and the business**. But it also needs to integrate with other governance bodies—spanning data, security, compliance, and automation—to avoid duplication, shadow AI, and fragmented oversight.

As adoption grows, so does the number of stakeholders. Platform admins, governance leads, champions, trainers, and support teams all play a role. Clearly defined roles and cross-CoE collaboration ensure accountability, foster alignment, and keep innovation tied to enterprise strategy

TIP

Many organizations use a RACI (Responsible, Accountable, Consulted, Informed) model to track actions and ownership as the CoE matures.

Designing Your Organization to Scale with Agents

Scaling AI and agents isn't just about deploying more models. It's about building the right organizational scaffolding—one that aligns vision, governance, Center of excellences, and execution across every layer of the business. A well-structured AI operating model ensures that strategic decisions flow downward with clarity, and operational insights flow upward with speed.

Here's how that structure typically plays out across four key groups:

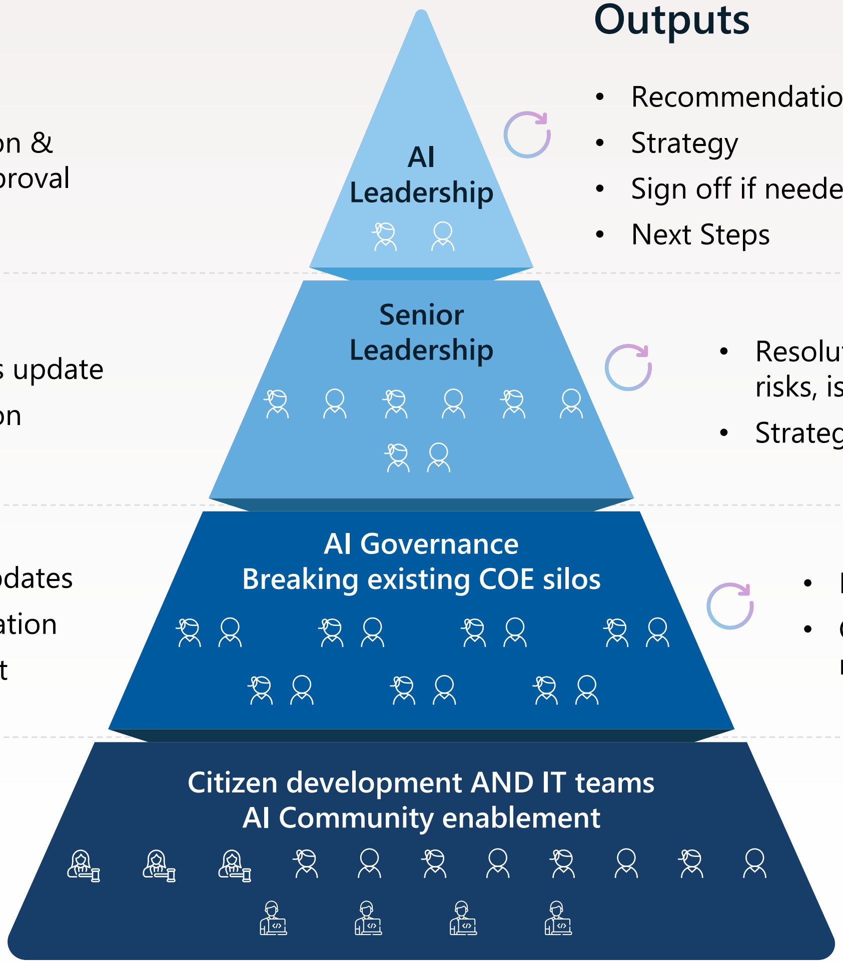
At the top is AI Leadership, operating on a quarterly cadence. This group is responsible for setting the overall vision for AI, agents, and making the strategic investment decisions. They don't manage day-to-day execution, but they do define what success looks like and where the organization should place its bets. Their inputs include project status updates, escalated issues, and quarterly performance reviews. In return, they provide strategic direction, approve major initiatives, and set the tone for responsible AI at scale.

Just below them is Senior Leadership, who meet monthly to translate vision into operational priorities. This group decides which AI and agent initiatives to prioritize, which partnerships to pursue, and whether to build or buy key capabilities. They rely on program-level updates and unresolved issues from the governance layer below. Their output includes tactical decisions, risk mitigation strategies, and recommendations that keep AI efforts aligned with business goals.

The weekly engine of AI and agent governance sits in the middle. This group is tasked with breaking down silos between your center of excellence and business units. They ensure that AI initiatives follow architectural standards, meet safety requirements, and deliver measurable business value. Their inputs are track-level updates and progress reports, and their outputs include issue resolution, cross-functional guidance, and architectural alignment. This is where operational rigor meets cross-team collaboration.

At the base of the structure are the citizen developers and IT teams, working on a daily and ad hoc basis. These are the people building and scaling agent use cases. They're closest to the work and need fast feedback loops, clear guardrails, and support to scale what works. Their inputs are real-time updates and escalations, and their outputs include validated use cases, surfaced blockers, and lessons learned that inform governance and strategy.

Designing Your Organization to Scale with Agents



	Inputs		Outputs	AI Accountabilities
Quarterly	- Project Status - Issues Escalation & Resolution Approval - Results wrap	AI Leadership	- Recommendations - Strategy - Sign off if needed - Next Steps	- Overall vision - Strategic decisions on AI investments
Monthly	- Program status update - Issues escalation	Senior Leadership	- Resolution or mitigation of risks, issues and blockers - Strategy recommendation	- AI Priorities for business - AI Partnerships - Build vs Buy decisions
Weekly	- Track status updates - Issues or escalation - Progress report	AI Governance Breaking existing COE silos	- Resolve issues - Cross-track guidance & recommendations	- AI Standards and safety - Architecture Governance - Bus. value proposition - Gen/AI use case entry point - Support use case scale up - Align to strategy - Responsible AI
Daily + Ad Hoc		Citizen development AND IT teams AI Community enablement	- Status updates - Issues or escalation - Progress report	- Design and Build AI - Reusable AI - AI diffusion and adoption - AI Skill Development

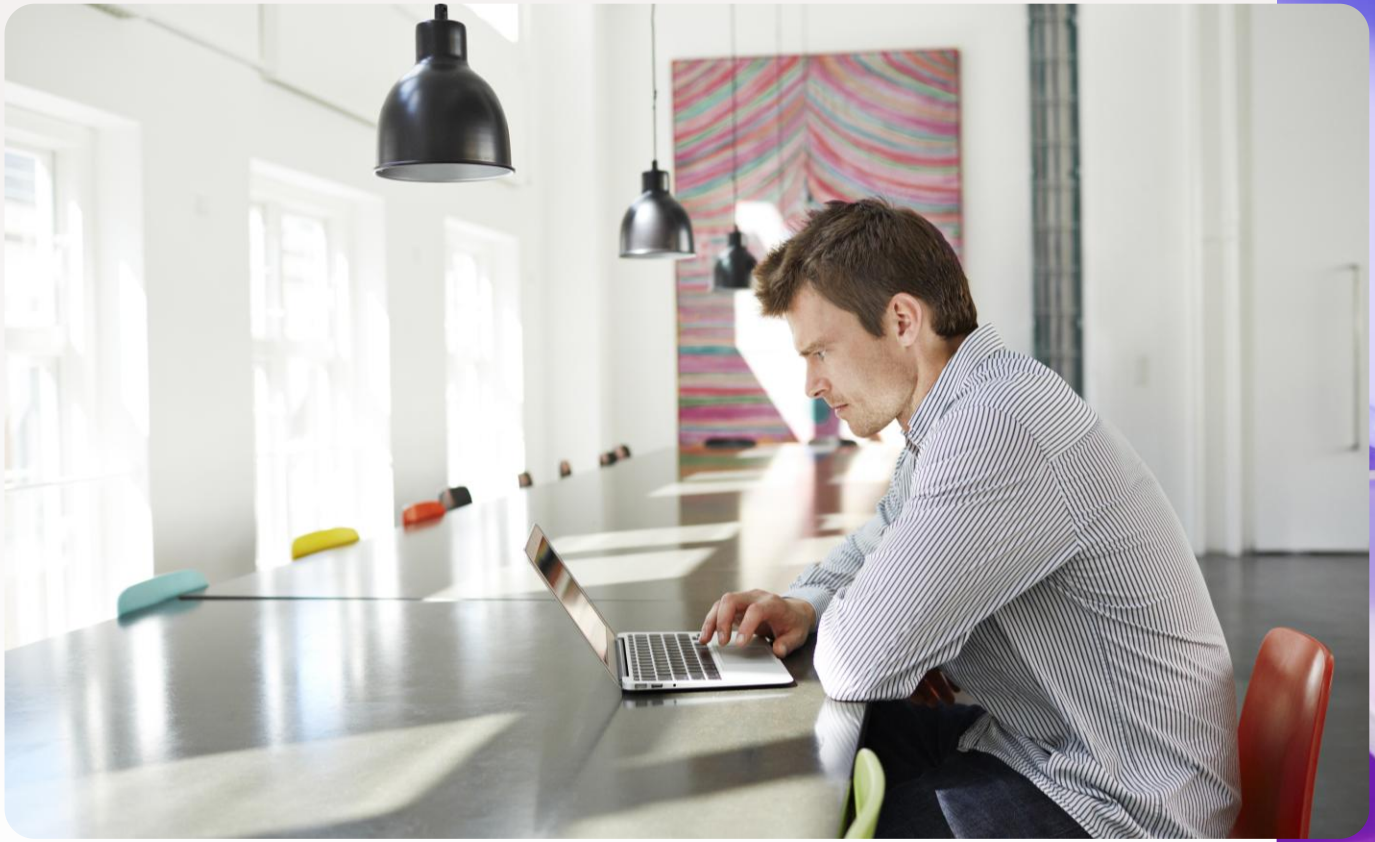
Emerging Roles for the Age of AI

As organizations operationalize agents and build the structures to support them, **CIOs will encounter a new wave of roles**—many of which didn't exist just a few years ago. Some of these roles may not even appear on today's org charts.

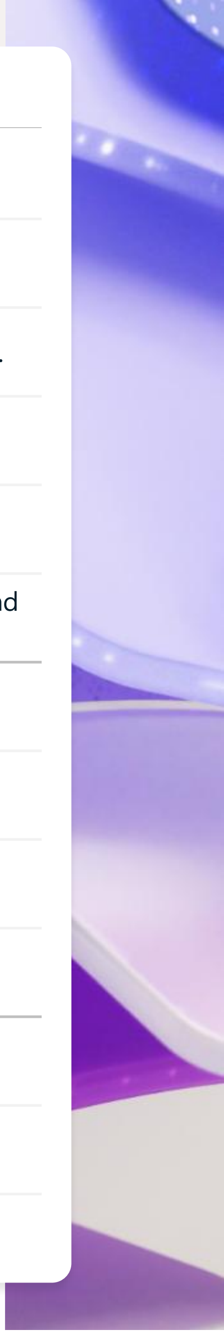
They're emerging in response to the unique demands of building, governing, scaling, and securing AI and agent systems responsibly.

This shift isn't just about hiring new talent. **It's about anticipating the capabilities your organization will need to lead with AI**—safely, strategically, and at scale. From ethics and risk to architecture and enablement, the center of excellence (CoE) becomes a hub for cross-functional leadership.

Some of these roles will evolve from existing functions, while others will be entirely new. Either way, the structure you put in place now will determine how effectively your organization can adapt to what's next.



Category	Role	What They Do
Strategic / Leadership	Chief AI Officer (CAIO)	Sets enterprise AI vision, aligns AI strategy with business goals, and leads the CoE.
	Chief Ethics Officer	Oversees ethical frameworks, bias mitigation, and societal impact of AI. Often collaborates with legal and compliance.
	AI Governance Lead	Defines and enforces AI governance policies, including transparency, accountability, and compliance.
	AI Risk Officer	Identifies and mitigates risks related to AI models, including hallucinations, drift, and regulatory exposure.
	Responsible AI Program Manager	Operationalizes responsible AI principles across teams, often driving training, tooling, and policy adoption.
	Chief Compliance Officer (CCO)	Ensures AI systems comply with internal policies and external regulations. Works closely with legal and audit teams.
Technical / Operational	AI Architect	Designs AI system architecture, including model orchestration, data pipelines, and integration with enterprise systems.
	AI Administrator	Manages AI tools, extensions, and environments (e.g., Copilot Studio, plugins, connectors).
	AI Security Specialist	Secures AI systems against threats like prompt injection, data leakage, and adversarial attacks.
	AI Ops Lead	Monitors AI systems in production, ensuring reliability, observability, and performance.
Enablement / Adoption	AI CoE Lead	Manages the CoE's charter, team, and intake process. Coordinates across business and technical stakeholders.
	AI Literacy & Enablement Lead	Drives internal education and change management to build AI fluency across the org.
	AI Community Manager	Builds and supports a network of AI champions, facilitates knowledge sharing, and promotes responsible innovation.



CIO Checklist

- ❑ Apply the Zoned Governance Model to match oversight to risk (CoE Lead / IT Governance)
- ❑ Enforce least-privilege access and connector policies (Security Admin)
- ❑ Isolate experimentation from production using environment routing (Platform Admin / DevOps)
- ❑ Define CoE roles and responsibilities using a RACI model (CIO / CoE Lead)
- ❑ Reinforce responsible development with maker banners and training (CoE Trainer / Compliance Officer)

SECTION FIVE

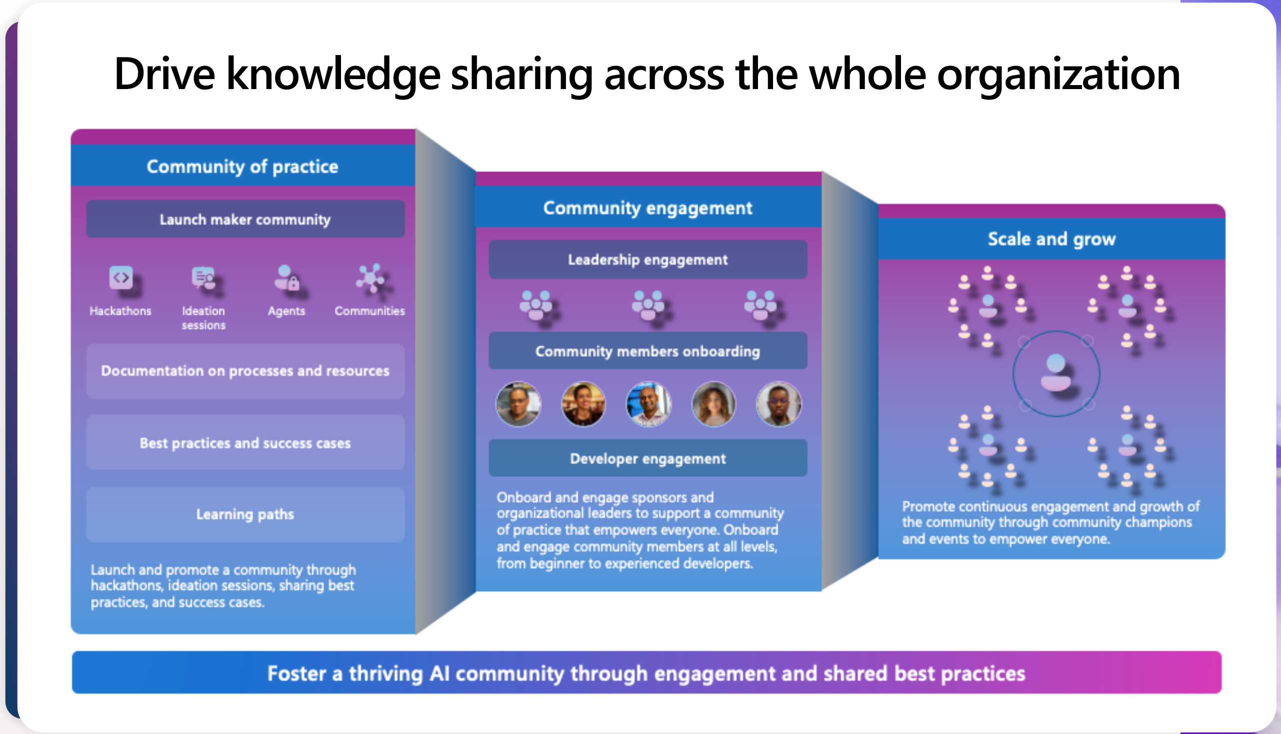
Community, Training, and Experimentation Drive Adoption

Community, Training, and Experimentation Drive Adoption

Achieving success with agents goes beyond technology implementation—it requires organizational readiness, skills development, and a culture that encourages experimentation and collaboration. CIOs play a crucial role in supporting this transition by ensuring people are informed and prepared, addressing challenges that often stem from organizational culture rather than technical barriers. Effective agent governance depends not only on policies and platforms, but on equipping personnel to contribute confidently and effectively.

Start with community. Communities drive collaboration, innovation, and growth. Learn why people join, how engaged communities benefit organizations, and the core factors for success. Learn more here.

Select Community champions. Identify early adopters from different departments to mentor peers and promote responsible adoption. These individuals model best practices, support others, and advance the community's goals and values. Learn more here.



Drive knowledge sharing across the whole organization

Launch and promote a community through hackathons, ideation sessions, sharing best practices, and success cases.

Onboard and engage sponsors and organizational leaders to support a community of practice that empowers everyone. Onboard and engage community members at all levels, from beginner to experienced developers.

Promote continuous engagement and growth of the community through community champions and events to empower everyone.

Foster a thriving AI community through engagement and shared best practices

Microsoft Digital shared:

We also flighted user awareness efforts to help employees understand not just how to use Copilot Studio, but also its implications for security, privacy, and Responsible AI. These campaigns included field readiness through Viva Learning, Copilot Champs sessions, newsletters, marketing campaigns through Viva Amplify, office hours, internal roadshows, and elite programs. Read more

Community, Training, and Experimentation Drive Adoption

Executive sponsorship is equally critical. When leaders actively support AI initiatives, it signals strategic importance, unlocks resources, and drives alignment across the organization. CIOs should work with business leaders to model the behaviors they want to scale. Learn more.

Next, invest in role-based training. Provide tailored learning paths for makers, admins, and business leaders. Use Copilot Success Kit and learning paths to accelerate readiness. Organizations can use Power Up, a free, virtual learning initiative designed to help non-technical individuals build future-ready skills in low-code development and Agents using Microsoft Power Platform and Copilot Studio. Learn how to establish training and upskilling here.

Pair training with support—create internal forums, helpdesks, and Teams channels to answer questions and share learnings.

To maintain progress, organize activities such as "Agent in a Day" workshops, hackathons, prompt-a-thons, and internal showcases to support skill development and identify additional use cases.

Encourage teams to share what they've built, what they've learned, and what others can reuse. Some organizations even create an internal Agent Marketplace—a catalog of reusable agents that promotes discovery, reuse, and cross-team collaboration.

This is a cultural shift. Treat community as infrastructure. Celebrate wins, share stories, and make agents part of how your organization learns and grows.

CIO Checklist

- ❑ Build organizational readiness by aligning culture, skills, and structure for agent adoption (CIO / HR Business Partner)
- ❑ Establish internal communities to drive collaboration, learning, and responsible experimentation (CoE Lead / Community Manager)
- ❑ Appoint community champions to model best practices and mentor peers (CoE Lead / Department Heads)
- ❑ Launch awareness campaigns to educate employees on agents and Responsible AI (IT Comms / Security & Privacy Office)
- ❑ Provide role-based training paths for makers, admins, and business leaders (Learning & Development / CoE Enablement)
- ❑ Create support channels and internal showcases to scale learning and reuse (CoE Enablement / IT Support)

From Strategy to Action: Get Started with Agent Governance

From Strategy to Action: Getting Started with Agent Governance

CIOs are uniquely positioned to lead the agent transformation by building and evolving on what already works. The governance models, CoEs, and controls you've established for Power Platform don't need to be reinvented, they need to be extended to incorporate agent autonomy, AI-driven decision making and responsible AI.

With the right foundation in place, agents have the potential to become trusted digital teammates when governed effectively: secure, compliant, and aligned with your business goals. **The opportunity is here—not just to manage risk, but to unlock innovation at scale.**

By taking these steps, CIOs can turn governance into a growth engine—scaling AI safely, accelerating adoption, and delivering real business value. If you've built a governance foundation, you're well-positioned to explore the next wave of innovation.

Further resources to get started

- Agent Governance Whitepaper
- Copilot Studio Implementation Guide
- Agent Success Kit
- Agents Cost Management eBook
- Agent Creator Community
- How to deploy transformational enterprise-wide agents: Microsoft as Customer Zero

Calls to action

1. **Extend Governance from Low Code to AI Agents**
   Build on your Power Platform foundation to create a unified governance model that spans agents, apps, and automation—ensuring consistency, reducing duplication, while adaptable to the evolving capabilities of agents.

2. **Operationalize Guardrails Through Structure**
   Use the Zoned Governance Model to scale safely, stand up a layered operating model to align oversight with execution, and define the emerging roles needed to govern agents at scale.

3. **Fuel Adoption with Community, Champions, and Reuse**
   Drive adoption by building a culture that supports experimentation and responsible innovation. Invest in role-based training, and internal communities that connect champions across the business. Equip teams with the skills, support, and space to learn, share, and scale what works.

Disclaimers
This document is provided for informational purposes only and does not constitute legal, regulatory, or compliance advice. Organizations should consult their own legal, compliance, and data protection teams to ensure alignment with applicable laws and internal policies.

The strategies, tools, and governance models referenced herein are based on Microsoft technologies and may not be suitable for all organizations, industries, or jurisdictions.

Any forward-looking statements are subject to change and should not be interpreted as commitments or guarantees.

Microsoft makes no warranties, express or implied, with respect to the information provided in this document. Use of the guidance is at your own discretion and risk.

< HOME