Agentic Control and Management

Our approach to governing, operating, and securing the *AI workforce*

We support you at every stage – starting with assessing where your organization is today, through to enterprise wide adoption of AI agents, delivered securely and with robust governance.

Why act now?

By the end of 2026, *40% of enterprise applications will embed AI agents.** Without governance, enterprises face shadow AI, identity chaos, audit gaps, and compliance exposure. Agentic governance provides a unified framework to deploy, secure, and manage AI agents at enterprise scale.

If agents become your digital workforce, you need a digital workforce department. That is what agentic governance delivers, powered by Microsoft Agent 365.

*Gartner Press Release, September 2025.

Capgemini helps you scale AI agents responsibly

Unified control plane

Capgemini sets up Agent 365 as your single command center for every AI agent in the enterprise. All agents are registered, tracked, and managed through one console: each with a defined blueprint, a business owner, and an IT sponsor. No more shadow AI: every agent is visible, every deployment controlled, every update orchestrated.

Embedded security and compliance

We embed enterprise-grade security at every layer: dedicated Entra ID identities for agents, DLP enforcement on all agent communications, and real-time threat detection via Defender, Sentinel, and Agent 365 Runtime Shield, mapped against OWASP agentic AI risks. Complemented by MS Foundry Control Plane it delivers deep observability, runtime controls, agent-specific evaluations, and red teaming capabilities, ensuring agents are not only governed, but engineered for reliability, safety, and performance at scale.

Shadow agents are discovered and either onboarded or retired.

Continuous monitoring and lifecycle management

Capgemini establishes a tight feedback loop so agent owners can continuously monitor performance, gather user feedback, and trigger refinements as needed. When an agent falls short, alerts go out and a structured refinement process is introduced. Every agent starts with defined success criteria and stays evergreen through regular reviews and structured improvement cycles. Your AI agents are never static: they continuously learn and improve.

Capgemini's differentiations

- Official Microsoft launch partner for Agent 365 — co-developed governance frameworks and accelerators
- Proven delivery of agent governance using Agent 365 and Microsoft 365 Copilot
- Structured approach to agent design, deployment, and lifecycle management
- Role-based enablement, AI Centers of Excellence, and change management in every engagement
- End-to-end delivery from strategy and assessment, through implementation, to managed operations: we build it, run it, and continuously improve it
- Governance as a foundational component of enterprise-wide agentic transformation with Agentic Industry Studio

Your journey to governed AI

A five phase path from assessment to enterprise wide governance

Assess

- Inventory AI agents, including shadow AI, across departments and hyperscalers; identify unauthorized tools and unmanaged deployments.
- Evaluate current identity management, DLP policies, threat detection, and observability capabilities against governance requirements.
- Clarify business objectives for AI. Identify use cases and pain points driving this initiative
- Score maturity across the three governance pillars: platform, security, and lifecycle, using Capgemini's Maturity Model.
- Identify regulatory and compliance gaps, security risks, and priority use cases for governed agent deployment.

Plan

- Configure and enable a single console across Agent 365, Copilot Studio, and Microsoft Foundry for registering, tracking, and managing all agents: Microsoft, third-party, and custom.
- Define agent blueprints: standardized Entra ID–based identity, ownership (business owner + IT sponsor), supported by Agent Owner and AI Steward roles and a governance committee, permissions, and access boundaries for every agent.
- Define security templates: predefined policies for DLP, logging, monitoring, conditional access, and acceptable use.
- Define the governed agentic lifecycle: governance gates, release readiness criteria, and structured feedback and review processes.

Deploy

- Stand up the Agent 365 Control Plane with centralized agent registry, Entra ID integration, Purview, Defender.
- Onboard 1–3 pilot agents through the governance gate: validated blueprints, assigned ownership, identity provisioned, security templates applied.
- Activate the observability layer: real-time telemetry, identity-tagged audit logs, and DLP enforcement.
- Enable threat detection and runtime defense: Defender, Sentinel monitoring agent behavior.

Operate

- Monitor agent compliance, performance, and security in real time via observability layer.
- Run continuous threat detection and shadow agent scanning to catch unauthorized tools and emerging risks.
- Conduct regular governance reviews with technical KPIs (uptime, error rate) and business KPIs (queries resolved, time saved, user satisfaction).
- Govern incident handling: define escalation tiers, fallback procedures, and equip teams with best practices and knowledge articles.

Scale

- Onboard agents under full governance, apply standardized blueprints and security templates across all departments.
- Formalize an AI Center of Excellence for long-term governance and AI agent management.
- Embed structured feedback loops: user feedback channels, performance-triggered retraining, and agent retirement processes for underperformers.
- Track ROI per agent: incidents prevented, time saved, cost savings, NPS, and revenue impact; governance drives value, not just compliance.

About Capgemini

Capgemini is an AI-powered global business and technology transformation partner, delivering tangible business value. We imagine the future of organizations and make it real with AI, technology and people. With our strong heritage of nearly 60 years, we are a responsible and diverse group of over 420,000 team members in more than 50 countries. We deliver end-to-end services and solutions with our deep industry expertise and strong partner ecosystem, leveraging our capabilities across strategy, technology, design, engineering and business operations. The Group reported 2025 global revenues of €22.5 billion.

Make it real.
www.capgemini.com

GIS_12.04.26_Soham