ARTIFICIAL INTELLIGENCE | ADVANCED | 2 DAYS

Governing AI Agents with Microsoft Agent 365

Once teams start building agents, most organisations discover they have no inventory of what exists or what it can reach. This course covers the Agent 365 control plane end to end: agent identity, registry and lifecycle, security posture through Defender, data governance through Purview, and the licensing constraints that shape what is actually available to you.

Why Agent Governance?

Agent sprawl is already happening

Low-code agent building means unmanaged agents appear faster than IT can track them.

Honest on licensing

Clear about which capabilities require which base licence before you plan around them.

Identity is the control point

Treating agents as first-class identities makes existing access policy apply to them.

Newest ground in the stack

Generally available since May 2026 and taught almost nowhere else.

What you'll be able to do

- Explain the observe, govern and secure model and what sits under each pillar
- Establish agent identity and apply access policy through Entra Agent ID
- Operate the agent registry and agent map to inventory what exists
- Assess agent security posture and remediate excessive permissions
- Apply Purview data governance, observability and communication compliance to agents
- Design an approval and onboarding workflow using policy templates
- Determine which capabilities your licensing actually entitles you to
- Define an operating model covering ownership, review and retirement

Who this is for

- Security architects and CISO-office teams
- Microsoft 365 and Entra administrators
- Compliance, risk and data governance leads
- Platform owners responsible for agent programmes

Curriculum

01 Agent Sprawl and the Control Plane Model

- Why agent proliferation outruns traditional IT asset management
- The observe, govern and secure model and what each pillar delivers
- What you already own versus what Agent 365 adds
- Scoping the problem in your own environment
- Building the internal case for a control plane

02 Agent Identity with Entra Agent ID

- Representing agents as identities in Microsoft Entra
- Applying conditional access, role-based and attribute-based controls to agents
- Access governance workflows and periodic review
- Least privilege for agents and scoping resource access
- **Hands-on:** assign identity and access policy to a sample agent

03 Registry, Agent Map and Lifecycle

- The agent registry as the single inventory of record
- The agent map and reporting for cross-environment visibility
- Ownership assignment and handling ownerless agents
- Rules-based governance and auto-deployment of approved agents
- Retirement, decommissioning and cleaning up abandoned agents

04 Security Posture with Microsoft Defender

- Agent security posture management across Copilot Studio and Foundry agents
- Detecting excessive permissions, misconfiguration and shadow agents
- Risk scoring, prioritised recommendations and attack path analysis
- Runtime threat detection and AI-specific attacks such as prompt injection
- **Hands-on:** triage a set of agent security findings

05 Data Governance and Observability with Purview

- AI observability in data security posture management
- Assessing agent data risk posture across Microsoft and non-Microsoft agents
- Extending DLP and sensitivity labels to agent interactions
- Communication compliance for human-to-agent and agent-to-human exchanges
- Retention and deletion policy covering agent activity

06 Licensing, Policy Templates and Operating Model

- Base licence prerequisites and what is not purchasable without them
- Which protections now sit behind an Agent 365 licence
- Policy templates for consistent controls at approval and onboarding
- Defining the operating model: who approves, who reviews, how often
- **Hands-on:** draft an agent governance policy for your organisation