Power CAT

POWER CAT KICKSTARTER

Govern and Secure Agents

Workshop overview & agenda

Description

In the Govern & Secure Agents workshop, you'll learn how to confidently govern and secure agents by understanding risks, defining roles, and setting priority initiatives to manage agent adoption, complexity, and security. Designed for Power Platform administrators and security teams, the workshop equips you with essential tools and product capabilities through real-world scenarios and guided simulations. You'll collaborate on interactive exercises, from identifying risks to mapping relevant features to creating actionable strategies. Collaborate across teams and apply responsible AI principles to address organizational needs that enable innovation, without compromising control.

15 min — Welcome and Introduction

Introductions and workshop logistics. Warm-up discussion on the risk your team perceives when getting agent governance wrong.

40 min — Success Framework – Identify Goals and Risks

Understand why governance is not (only) risk management. Define your agent adoption goals and establish a shared view of success across your team. Through interactive discussions, identify risks that hinder achieving your agent's adoption goals. Learn about People, Process and Tools – the primary pillars to balance across innovation, governance and security

40 min — Responsible AI Practices - Navigate Agent Risks

Learn to move from reactive problem-solving to proactive risk management using Microsoft's Responsible AI (RAI) principles applied to real-world examples. A comprehensive guide to help you understand, identify, and respond to risks associated with AI systems. Through an interactive exercise you determine which RAI principles are most affected by the risks you've identified, helping you align your strategy with ethical and responsible practices.

15 min — Break

1 hour — Agent Governance Tools

Discover the tools available to support your Agent Governance Strategy. Are you struggling to track who's building agents, where they're shared, or how to manage sprawl and shadow IT, or how AI is being used across your organization? If you're asking these questions, you're not alone. In this module, through demos and click-through simulations you will get hands-on experience managing agents.

1 hour — Lunch Break

45 min — Environment Management and Strategies

Learn to design an effective environment strategy using real-world examples, zoned governance frameworks, and data policies to manage your environments. Understand key decisions in managing environment requests, defining agent-safe guardrails, and evaluating impact of Data policies. Use practical scenarios to test your strategy and build an action plan for identifying gaps.

45 min	**Agent Security Tools**
	Dive deeper into the tools available on the platform for securing your agents. This module provides individualized risk insights, actionable guidance, and an overview of security foundations and data policies to address challenges such as data leaks, unauthorized access, compliance requirements, and external threats.
15 min	**Break**
75 min	**Activate Goals with Role Clarity and RACI assignment**
	Governing agents require a coordinated effort across multiple teams. In this module you'll explore common agent governance and security roles and work collaboratively to co-create a prioritized initiatives roadmap using a RACI (Responsible, Accountable, Consulted, Informed) matrix. Building on insights from previous exercises, you'll prioritize initiatives by evaluating features, gaps, and opportunities. Determine which teams and roles need to be involved and develop an action plan to address security gaps and enhance agent governance.
15 min	**Q&A and Wrap up**
	Wrap up the session with survey, key takeaways, ownership and timelines for next steps. Share the resources available for participants including the tools for mitigating risks. Open for Q&A to address any parking lot questions.