Advanced Agent creation

Measure Twice, Build Once:
Designing Robust AI Agents with Copilot Studio

Bülent Altinsoy

Katerina Chernevskaya

A bit about Bülent

Speaker, Blogger, Podcaster, YouTuber, Mentor, Community Lead

Microsoft MVP — Microsoft Most Valuable Professional

Microsoft MCT

Community

Job Title

Solution Architect ***Power Platform & Copilot Studio***

Company

avanade

Fun Fact

"You will never get a job because of your poor English skills"

Hobbies

Family
Basketball
Electronic Music

LI: buelent-altinsoy
YT: @MultiDataverse

Blog: **thatalohaguy.substack.com**

A bit about Katerina

Contributor and collaborator in ***Microsoft PnP****, regular speaker who somehow keeps saying "yes" to more events*

Community

aka.ms/powerplatform-samples

Job Title

Power Platform Architect

Company

KPMG

Fun Fact

"Our family doesn't do sports... we collect certifications. Two MVP/MCT, one MCT, and a 10y.o. already deep into IT"

Hobbies

Studying new tech for "fun", because apparently that counts as a hobby now

/in/katerinachernevskaya

PICK YOUR FLAVOR:
COOKIE FOR QUICK WINS,
GINGERBREAD FOR ENTERPRISE DREAMS

COLLABDAYS OSLO

Schedule

09:00 – 10:00 Brain Boot-Up

10:00 – 10:15 Break

10:15 – 12:30 Deep Dive

12:30 – 13:30 Lunch

13:30 – 15:15 Post-Lunch Survival Mode

15:15 – 15:30 Break

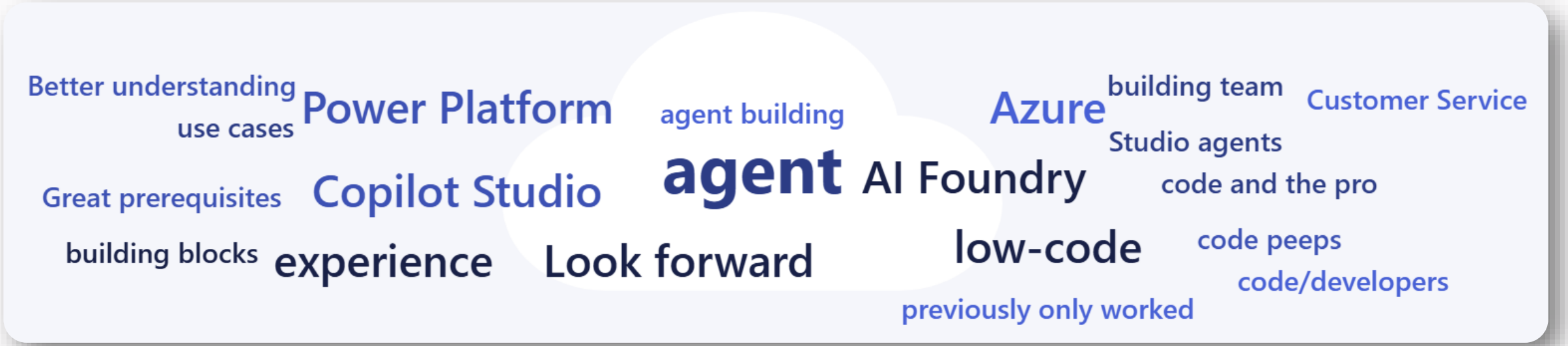
15:30 – 17:00 Victory Lap & Wrap-Up

Labs

- Create Agent
- Extend agent with tools, triggers, topics
- Deploy Azure resources
- Configure AI Search and integrate with Agent
- BYOM
- Evaluation
- Agent in Azure AI Foundry

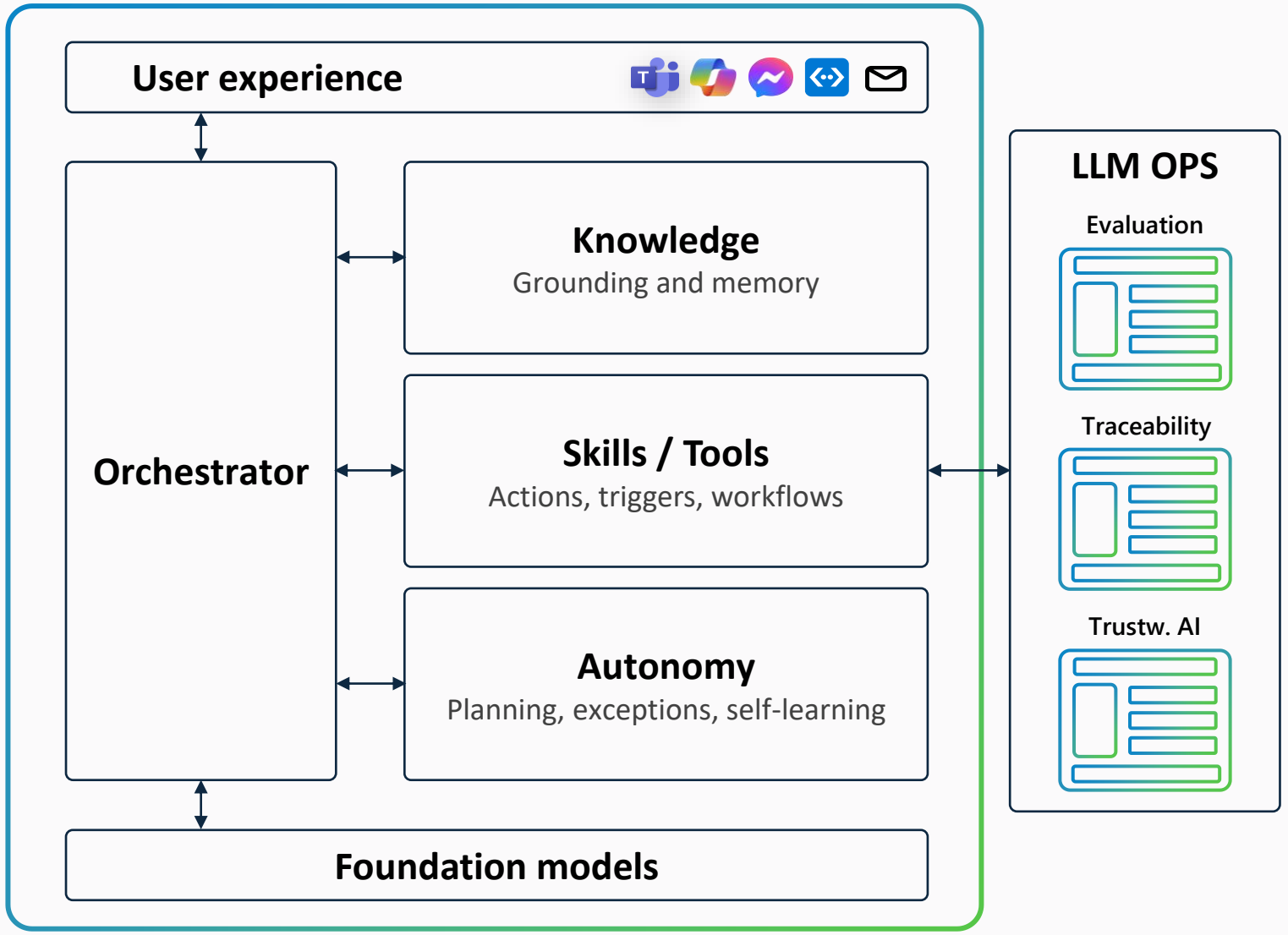
Workshop Lab Guidelines

- **No rush, no pressure** – the goal isn't to finish every lab today. You'll keep all materials afterwards.
- **Focus on principles** – what matters is understanding how to design AI solutions. Open discussions are welcome.
- **Flexibility encouraged** – you're free to experiment and build your own agents, though we recommend starting with the lab steps first.
- **Ask for help** – if you get stuck, let us know. We're here to support you.
- **Set your own pace** – some move fast, others prefer to go deeper. Both are perfectly fine.
- **Stay curious** – the labs are just a starting point. Use them as a playground for exploration.
- **Support each other** – share discoveries, ideas, and insights with the group.

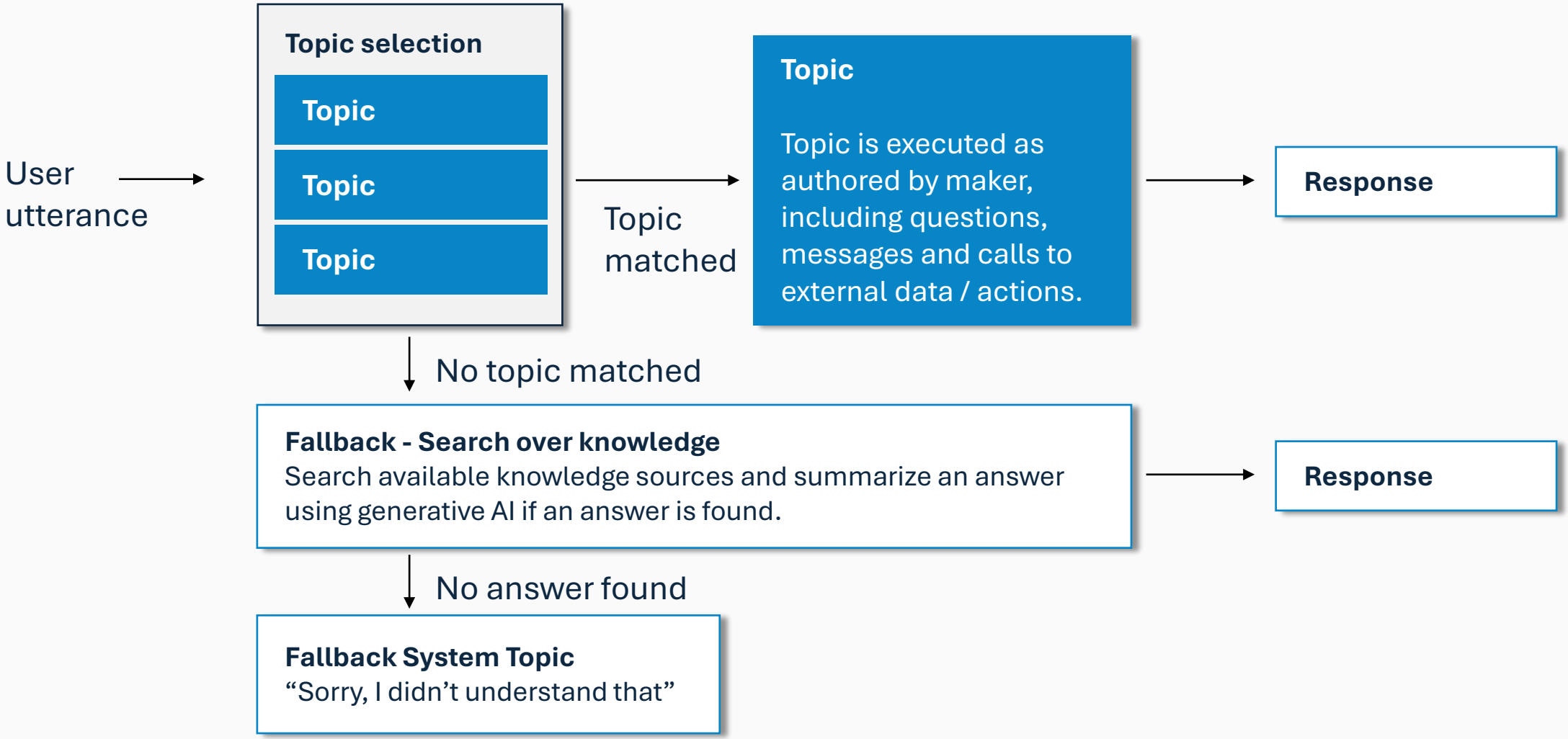

Better understanding
use cases
Power Platform
agent building
Azure
building team
Customer Service
Studio agents
agent
AI Foundry
Great prerequisites
Copilot Studio
code and the pro
building blocks
experience
Look forward
low-code
code peeps
code/developers
previously only worked

Agents anatomy

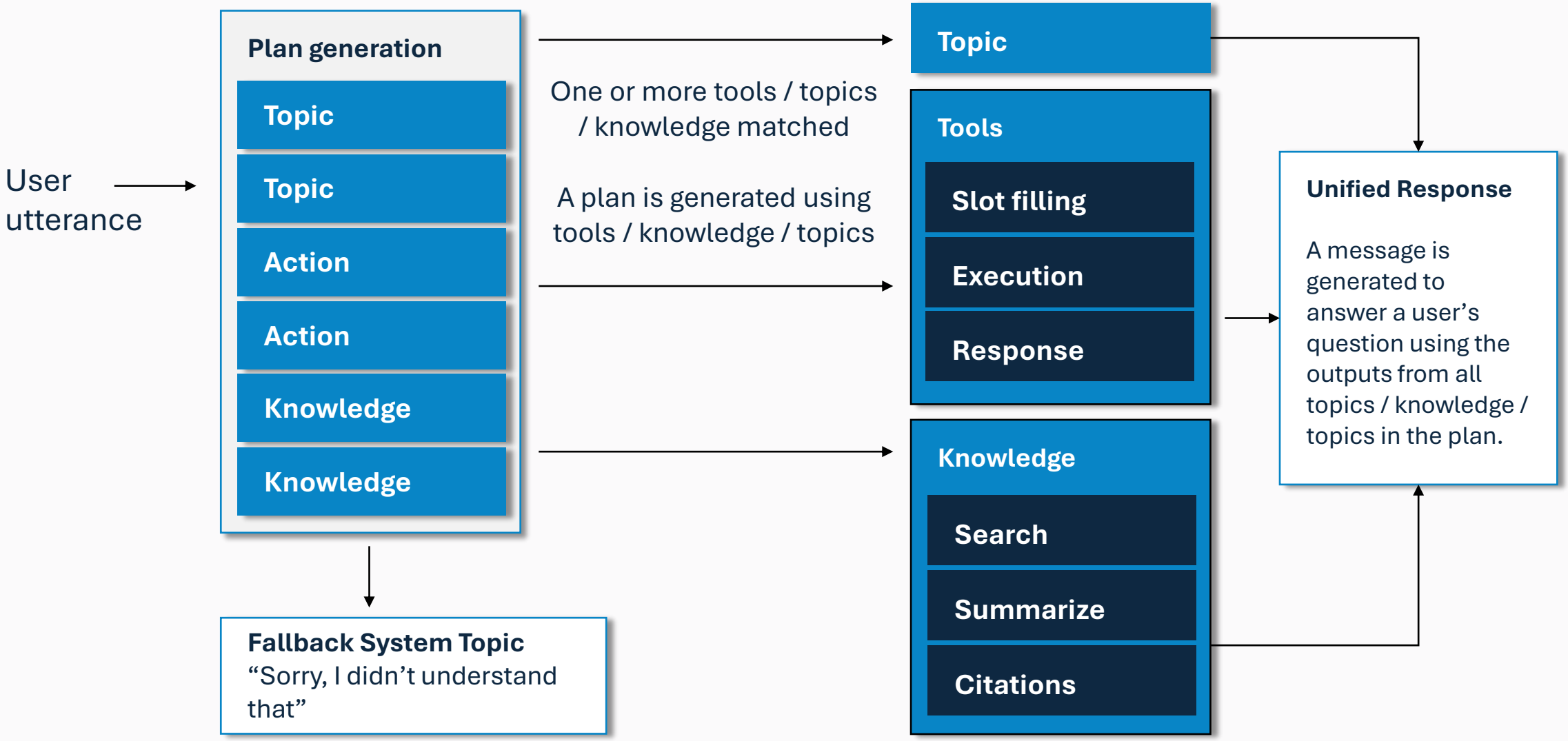
Agents anatomy



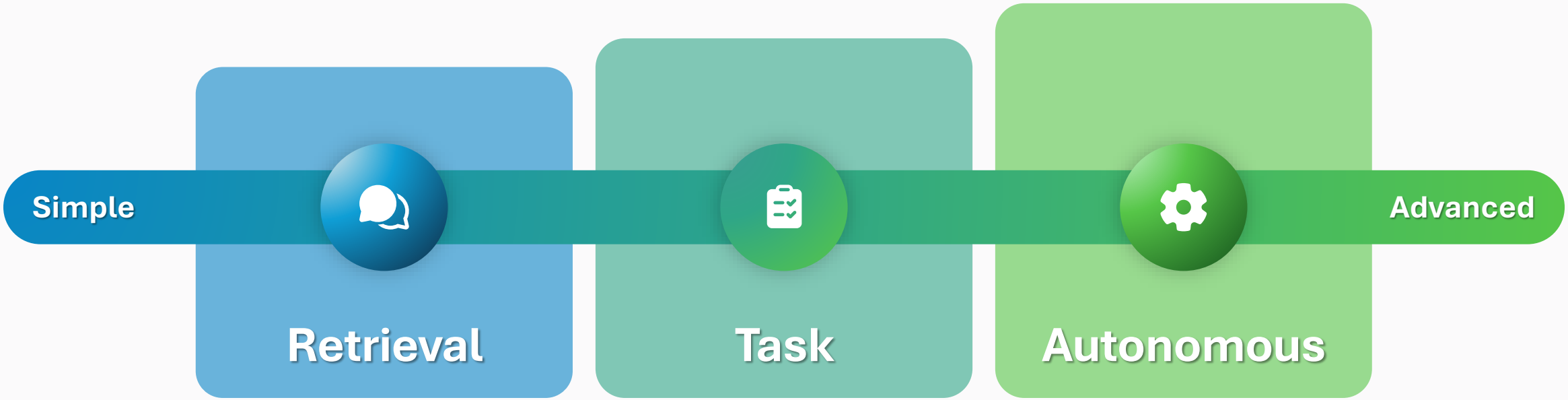
Classic orchestration



Generative orchestration



Agents are apps that use AI to reason, plan, connect to systems and complete tasks working alongside or on behalf of a person, team or organization



Agents vary complexity and capabilities depending on your need

People + Copilot + Agents

Levels of AI transformation

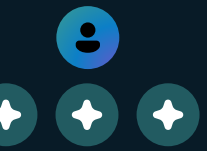
Level 1

Humans with assistants

Every person is augmented by AI that understands their job

Level 2

Human-led agents



Every team includes AI agents, managed by humans, that complete tasks autonomously

Level 3

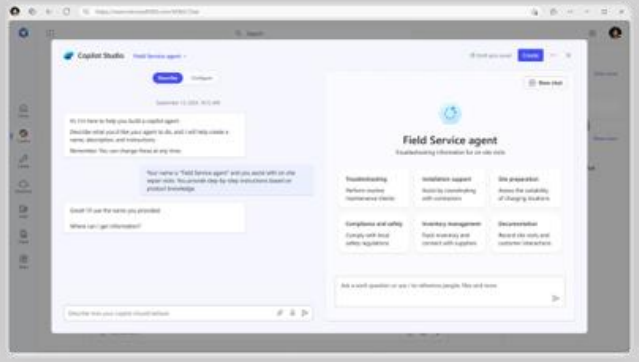
Teams of Humans and Agents

Humans set direction and AI agents run entire teams or departments, checking in as needed

A range of tools for agent creation

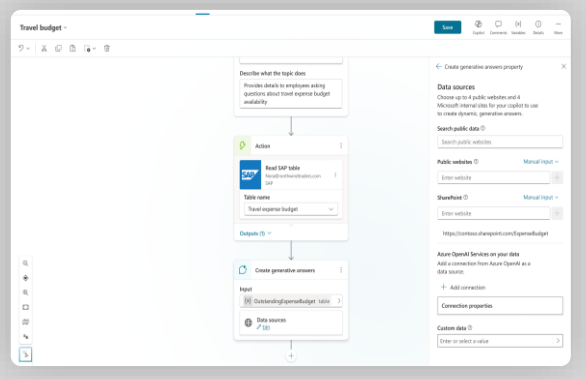
No code — Pro code

For end users



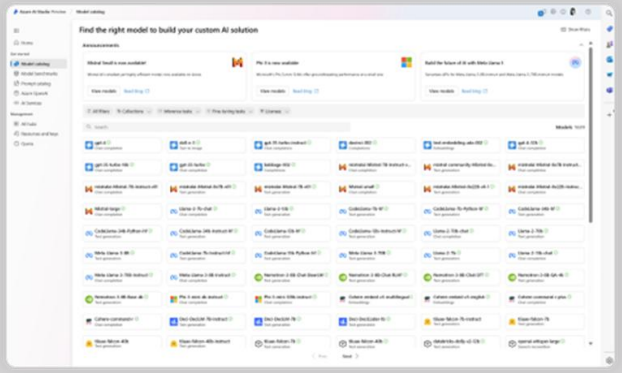
Agent builder

For makers



Copilot Studio

For developers



Copilot Studio, Azure AI Foundry, M365 Agents SDK

Data protection, agent sharing & usage limits, and reporting & cost management


COLLABDAYS OSLO
Copilot Studio Architecture
API-based clients
Copilot Studio standard clients
Standard Web Chat widget
Power Apps chat control
Power Pages chat control
Custom clients
Bot Framework Web Chat
Custom apps & chat widgets
Server-to-server
Custom middleware
Azure AI Bot Service channels (Telegram, WeChat, etc.)
3rd-party engagements hubs
Microsoft Teams
Facebook Messenger
WhatsApp (2025)
Slack (2025)
Dynamics 365 Contact Center (voice/text)
Microsoft 365 Copilot
Azure AI Bot Service
Bot Framework bot
Bot Framework skill
Runtime
Native channels
Direct Line (HTTP / WebSocket)
Direct-to-Engine (HTTP / SSE)
Microsoft Teams
Facebook
WhatsApp (2025)
Slack (2025)
Dynamics 365 Omnichannel
Microsoft 365 Copilot
Agent as a skill (private preview)
Integrations
HTTP requests
Power Platform connectors
Power Automate cloud flows
AI Builder prompts
Bot Framework skills
ALM
Power Platform solutions
CI/CD (pipelines/ADO/GitHub)
Dialog management
Topics
Nodes
Actions
Power Fx
Voice
Multilingual
Generative actions
AI-wrapper for integrations
Inputs
Outputs
Security
Web channel security (secret)
End-user authentication
No authentication
Native / Custom auth
Power Platform DLP policies
Authentication settings
Enabled channels
Enabled knowledge sources
Enabled connectors
Microsoft Purview audit logs
VNET / IP firewall (2025)
Triggers (autonomous agents)
Language understanding
Classic
Built-in NLU
Bring your own NLU model
Generative orchestration
Generative answers
Query rewriting
Knowledge search
Websites
Custom data
Files
SharePoint
DV Tables
Graph
Federated Knowledge
Azure AI Search
Summarization
Native
BYOM (2025)
AI general knowledge
Standard analytics
Technical telemetry
Conversation transcripts
Azure AI Language
Conversational Language Understanding (CLU)
Microsoft 365 Graph
Enhanced search results
Graph connectors
Azure AI Search
Vectorized search indexes
Azure AI Foundry
LLMs, SLMs, Fine-tuned models
Azure Monitor
Application Insights
Azure Storage
Data lake
Azure Synapse Analytics
Workspace
Microsoft Entra ID
App registration

Ignite 2025: Enabling the Frontier Firm

M365 Copilot

Microsoft Agent 365
The control plane for agents

Copilot Studio

Work IQ | Fabric IQ | Foundry IQ

COLLABDAYS OSLO

NO SILVER BULLET.

INTELLIGENT AGENTS DEMAND INTELLIGENT CHOICE.

Lab time

- Check prerequisites
- Create first agent with knowledge
- Add tool, trigger, topic

INSPIRE
A Framework for Successful Implementations

- Microsoft Cloud Adoption Framework (CAF)
- Power Platform Well-Architected Framework
- Azure Well-Architected Framework
- Power Platform ALM Guidance
- Microsoft Responsible AI Standard
- Administering and Governance Agents
- Copilot Studio Governance and security Guide

COLLABDAYS OSLO

Security Survivor

Game time

Microsoft Copilot Studio and Azure = Better together

Bring your own model
Generate responses or run specific tasks using your own standard or fine-tuned models from Azure AI Foundry.

Bring your own index
Vectorize content in Azure AI Search and surface the content for your agents as standard knowledge sources.

Bring your own natural language understanding model
Train your own models for intent recognition and entity extraction

Bring your own CI/CD pipeline
Configure pipelines in Azure DevOps to automatically deploy and source-control your agents

Bring your own agent with Agent2Agent (A2A) and more
Use the Microsoft 365 Agents SDK, the Azure AI Bot service, any compatible A2A agents.

Bring your own AI tools and data with Model Context Protocol
Create next-generation AI tools and data sources that can be consumed from agents through the MCP protocol

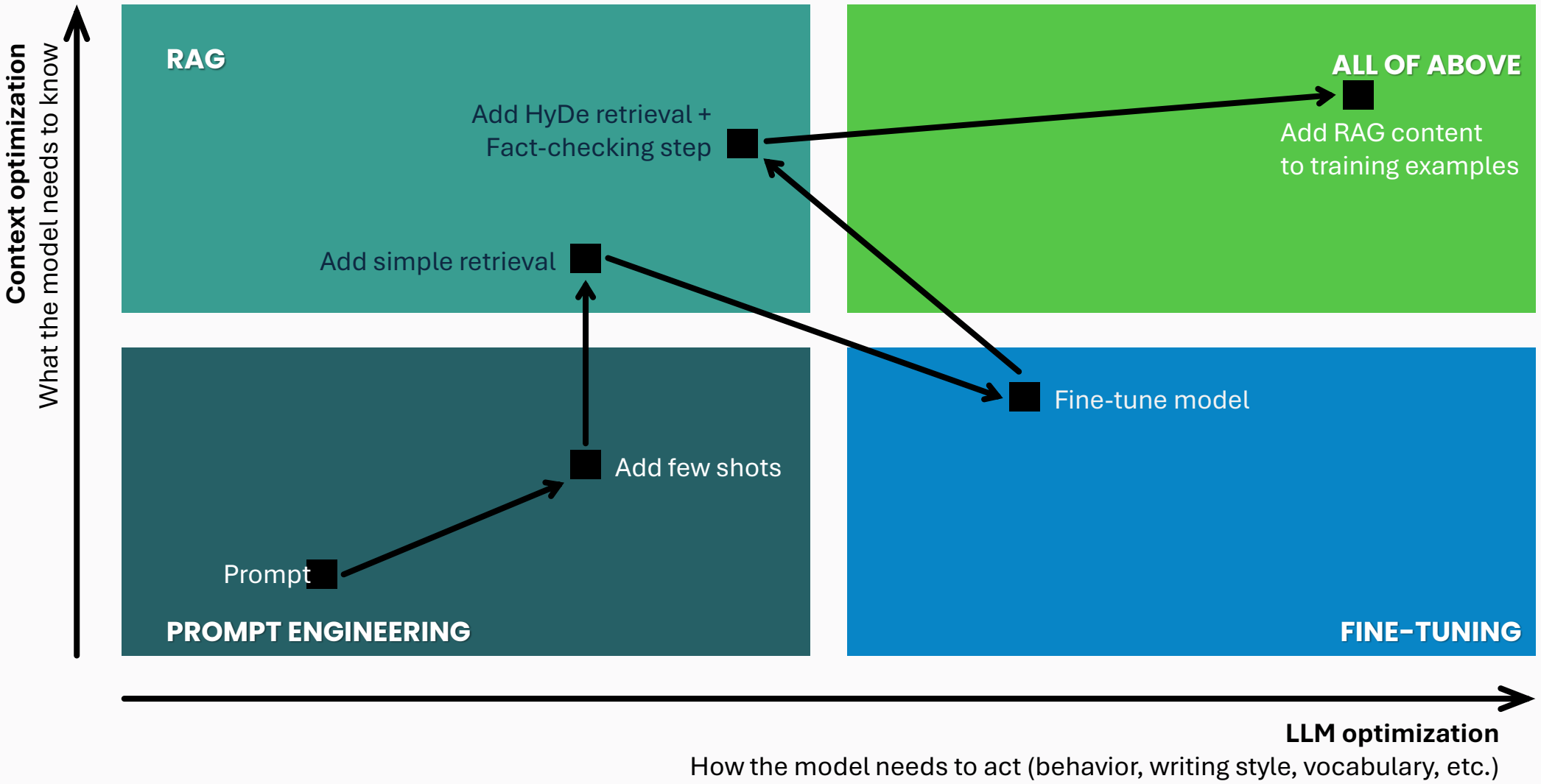
Isolate your agents and APIs
Isolate your agents with subnet delegation into your virtual networks for outbound connectivity, and setup IP firewalls and continuous access evaluation for inbound.

Monitor your agents
Stream technical telemetry for standard and custom events and integrations into Azure Application Insights.

Bring your own data lake
Move conversation transcripts to a lake for long-term storage and usage and custom analytics.

Bring your WhatsApp and voice channnels
From Azure Communication Services and with D365 CC for a voice telephony channel (IVR scenarios)

LLM accuracy improvement



THE PROCESS OF RETRIEVING CONTENT TO AUGMENT YOUR LLM'S PROMPT BEFORE GENERATING AN ANSWER

RAG helps AI provide accurate answers based on real data

1️⃣ **Search** 🔍 – AI looks through knowledge sources (indexes) using an optimized query.

2️⃣ **Retrieve** 📄 – AI fetches the most relevant text snippets.

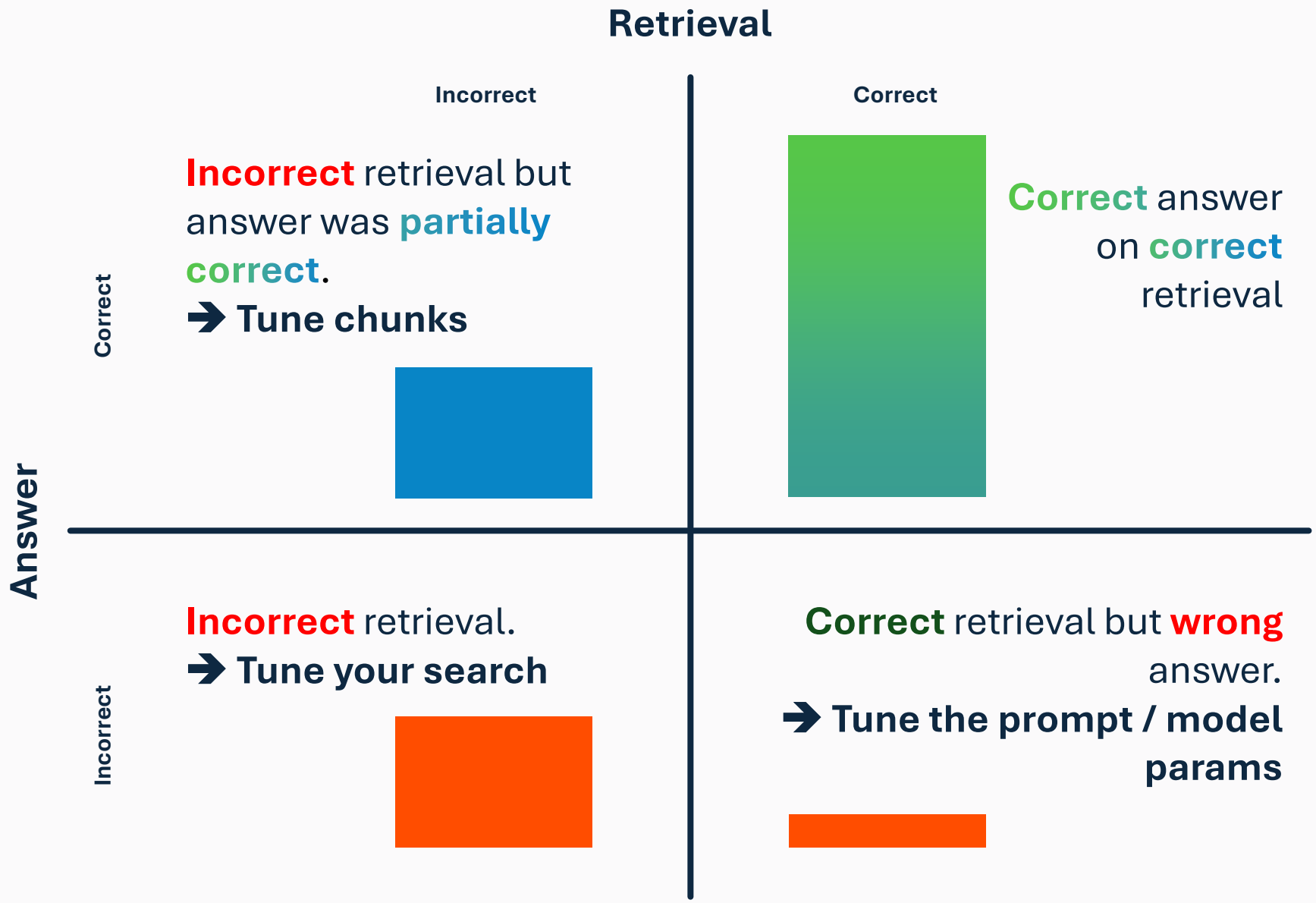
3️⃣ **Summarize** ✍️ – AI generates a fact-based response with citations.

What RAG Does NOT do:

❌ **Not for deep document analysis** like:

- **Comparing two long documents**
- **Checking contract compliance against policies**

💡 **Instead, it retrieves and summarizes data, keeping responses grounded in facts!**


Retrieval
Incorrect
Correct
Answer
Correct
Incorrect
Incorrect retrieval but answer was partially correct.
➔ Tune chunks
Correct answer on correct retrieval
Incorrect retrieval.
➔ Tune your search
Correct retrieval but wrong answer.
➔ Tune the prompt / model params

COLLABDAYS OSLO

RAG Reality Check

Game time

Lab time

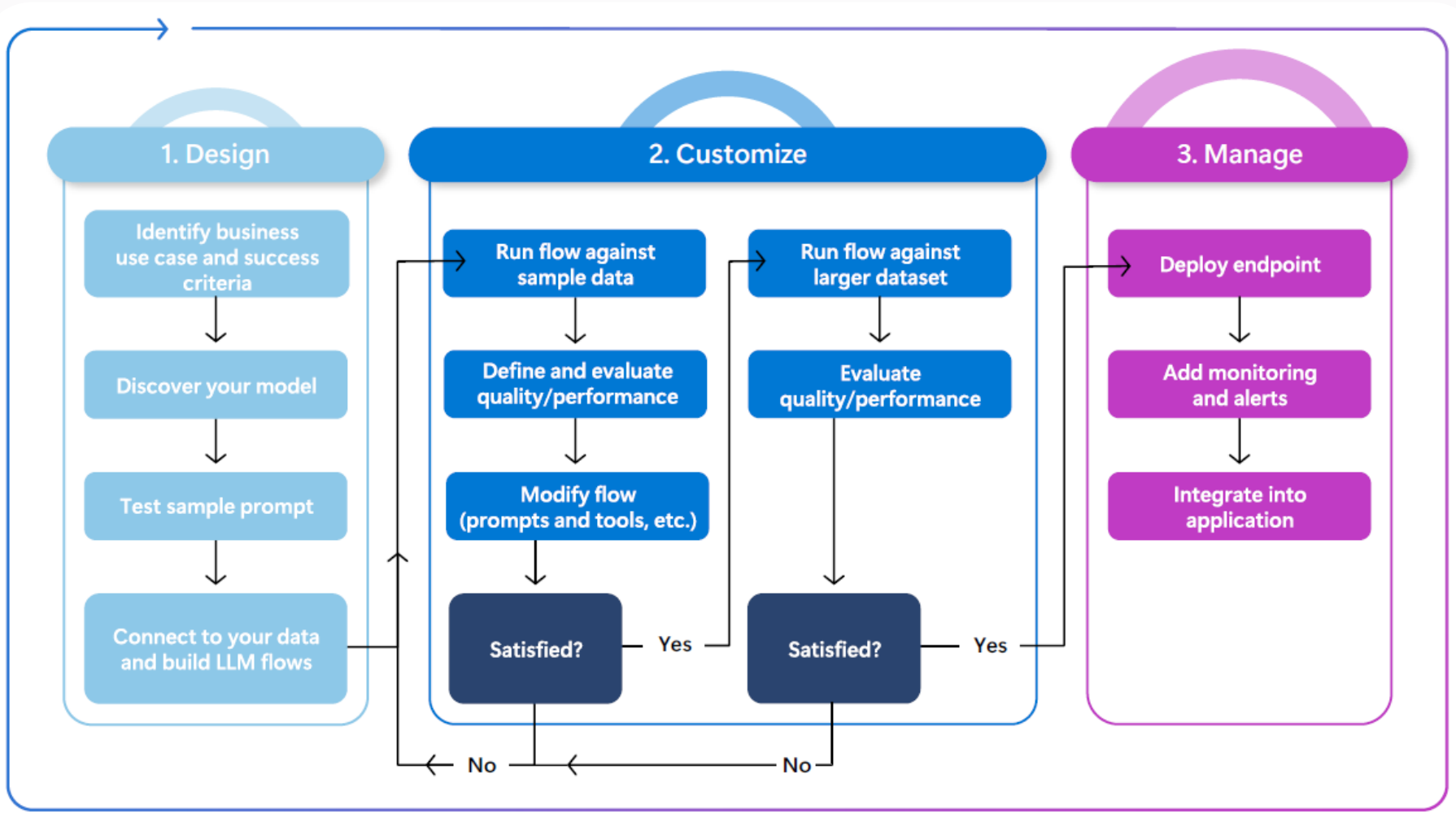
- Deploy Azure resources
- Configure Azure AI Search
- Integrate index into Copilot Studio

HOW DO YOU TYPICALLY TEST IF A MODEL OR APPLICATION IS WORKING AS INTENDED?

At least **30%** of generative AI (GenAI) projects will be abandoned after proof of concept by the end of 2025, due to **poor data quality**, **inadequate risk controls**, **escalating costs** or **unclear business value**, according to Gartner, Inc.

https://qrco.de/gartner-article

Evaluation loop



Copilot Studio Kit

The **Copilot Studio Kit** is a comprehensive set of capabilities built for Microsoft Copilot Studio. The kit includes features such as

📊 **Conversation KPIs** – Gain deeper insights into long-term agent performance with structured analytics.

🧪 **Test Automation** – Batch test custom agents with multiple validation methods.

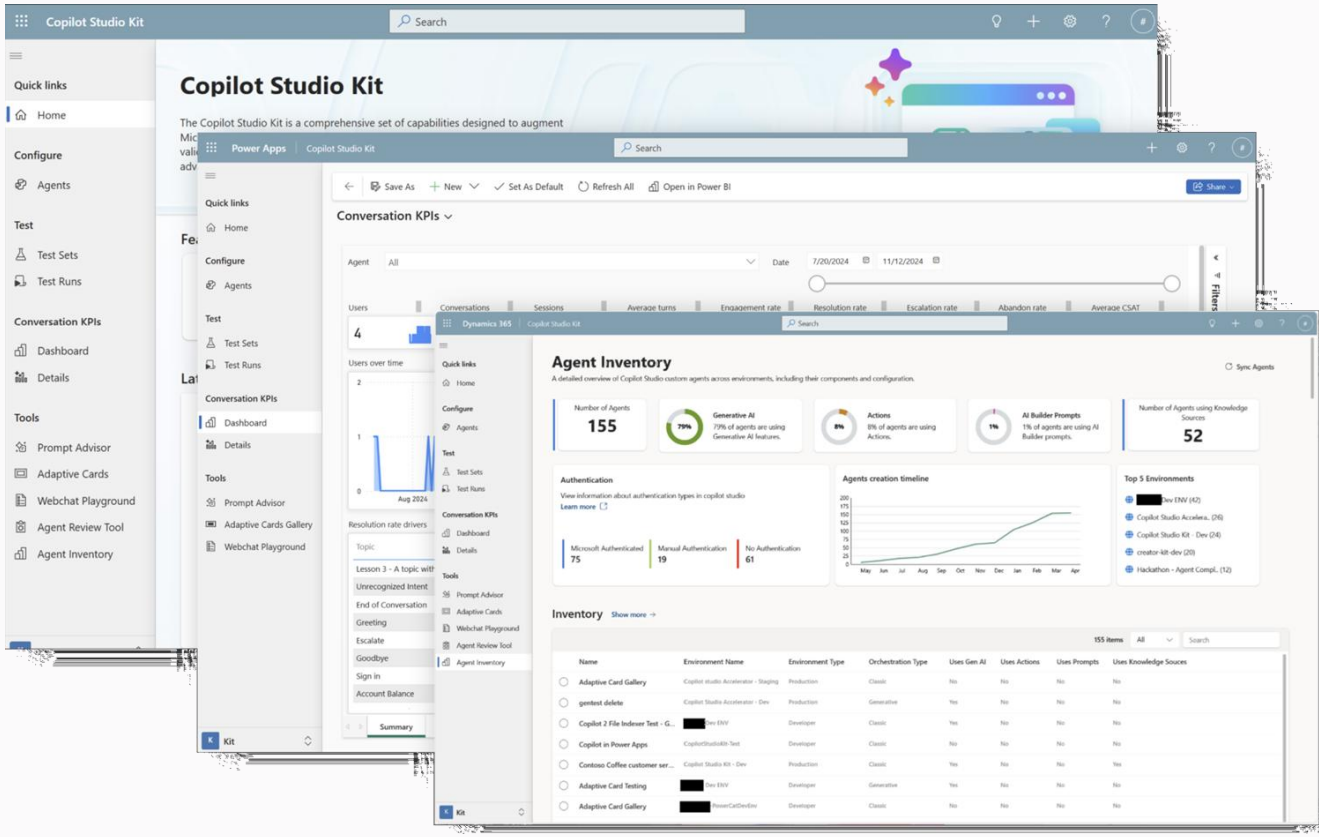
📈 **Agent Inventory** – Get tenant-wide visibility to all the Copilot Studio custom agents in the organization, across environments.

🛠️ **Agent Review Tool** - Static analysis of copilot studio agents from solution. Detecting anti-patterns and suggesting mitigation.

🗂️ **SharePoint Synchronization -** Selectively synchronize knowledge from a SharePoint site as local knowledge of your custom agent.

💬 **Webchat Playground** – Customize the look and feel of your webchat with an easy-to-use interface.

🧩 **Adaptive Cards Gallery** – Access a set of pre-built Adaptive Card templates for custom agents



➡️ https://aka.ms/DownloadCopilotStudioKit (AppSource)
➡️ https://aka.ms/CopilotStudioKit (GitHub + Docs)

COLLABDAYS OSLO

Eval Showdown

Game time

Lab time

- BYOM
- Evaluation
- Azure AI Foundry Agents

Securing and Governing Agent

Streamline governance at scale

Secure

Built to Stay Safe

Runtime Protection

Compliance and Privacy

Data Protection

Control

Environment Strategy
Maker onboarding

Certification Workflows

Cost Management

Track & Refine

Readiness and Adoption

Business value & ROI

Zone management

Posture optimization

ALM Golden Rules

- ✓ Work in the context of solutions
- ✓ Create separate solutions only if you need to deploy components independently.
- ✓ Use a custom publisher and prefix.
- ✓ Use environment variables for settings and secrets that change across those.
- ✓ Export and deploy solutions as managed, unless setting up a dev environment.
- ✓ Don’t do customizations outside of dev.
- ✓ Consider automating ALM for source control and automated deployments.

COLLABDAYS OSLO

Questions & Answers

COLLABDAYS OSLO

Thank You!