



Power CAT ***AI WEBINARS***

Building an AI-ready organization

Meet your hosts



Ashleigh Nyazema

Program Manager

Power CAT



Vasavi Bhaviri Setty

Senior Program Manager

Power CAT



Ken Auguillard

Principal Program Manager

Power Platform



Intro Poll – What future sessions would you like to see?



Poll

Poll link: aka.ms/AiWebinars/Polling

Passcode: PowerCAT



Power CAT **AI** Webinars

Evolving Governance



Outline

- Governance overview
- Environments
- Zoned Governance
- Connector policies
- Managed Security
- Key takeaways
- Q&A



Microsoft Power Platform

The most complete low-code platform



Copilot Studio

Customize & create agents



Power Apps

Application development



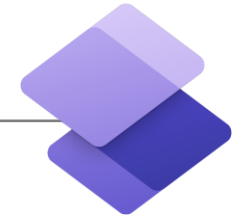
Power Automate

Process automation



Power BI

Business analytics



Power Pages

Business websites



**Data
connectors**



AI Builder



**Microsoft
Dataverse**



Power Fx



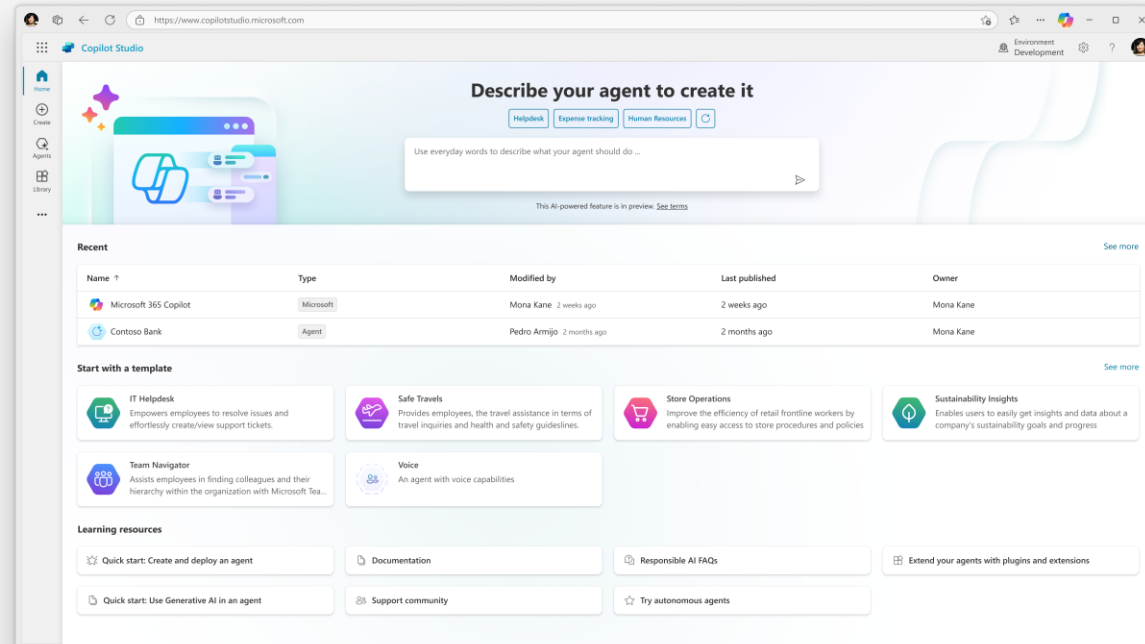
**Managed
Environments**





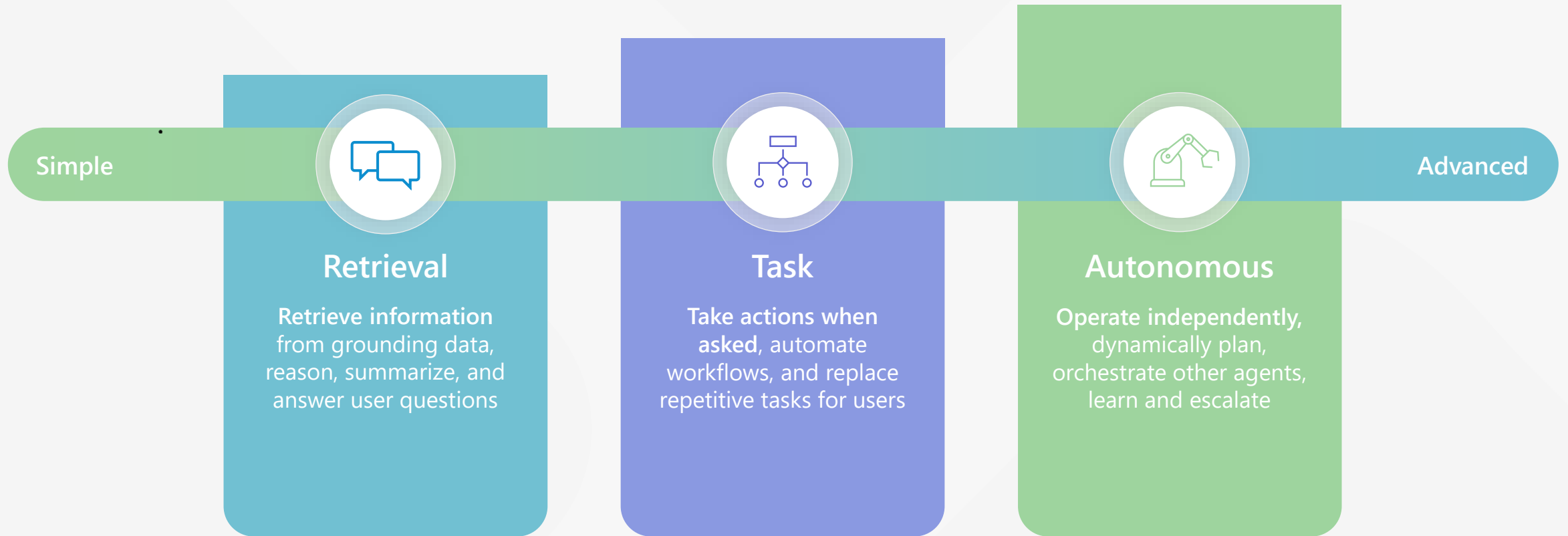
Copilot Studio

Copilot Studio is a low code tool for **building agents** and **extending Microsoft 365 Copilot**.



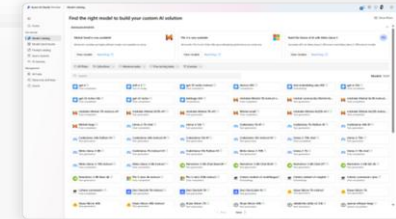
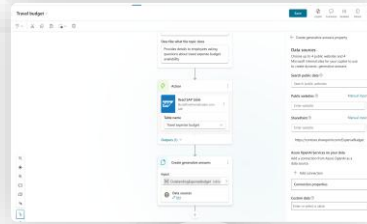
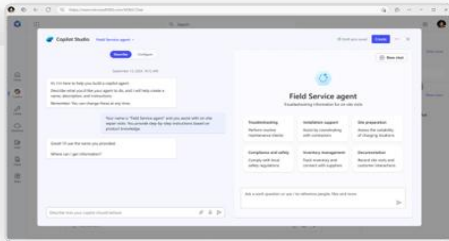
- ✓ Meet your users where they already are
- ✓ Access everything in one place
- ✓ Automate your workflows
- ✓ Integrate with your external apps
- ✓ Connect to your data in Microsoft 365

Spectrum of agents



← Agents vary in levels of complexity and capabilities depending on your need →

Advanced agents require more advanced governance and security



Simple



Agent builder

For End Users



Copilot Studio

For Makers



Copilot Studio + Azure AI

For Developers

Advanced

Knowledge

←···· Microsoft Graph Your Business Data ···→

Actions

←···· Retrieval Only Task / Autonomous ···→

Channels

←···· Microsoft 365 Only Multiple Internal & External Channels ···→

..... Increasing advanced governance and security needs
throughout agent lifecycle

1. Development & Testing

2. Deployment

3. Optimization



What are the risks of getting **AI Governance** wrong in your organization?



Poll

Poll link: aka.ms/AiWebinars/Polling

Passcode: PowerCAT



Top security and governance concerns with generative AI

Data oversharing
and data leaks

80%

of leaders cited leakage of sensitive data as their main concern¹

Identification of
risky AI use

41%

of security leaders cited that the identification of risky users based on queries into AI was one of the top AI controls they want to implement²

AI governance and
risk visibility

84%

Want to feel more confident about managing and discovering data input into AI apps and tools²

1. First Annual Generative AI study: Business Rewards vs. Security Risks, Q3 2023, ISMG, N=400


2. [Microsoft data security index 2024 report](#)




What do you consider to be the single greatest risk associated with AI?




Open text Poll ☒ 10 Response  9 Participant

• data leak  9

• Misinformation  7

• Trust  2

• data security  1

• How Data is handled  1

• Wrong action based on Agents actions/responses

• data exfiltration

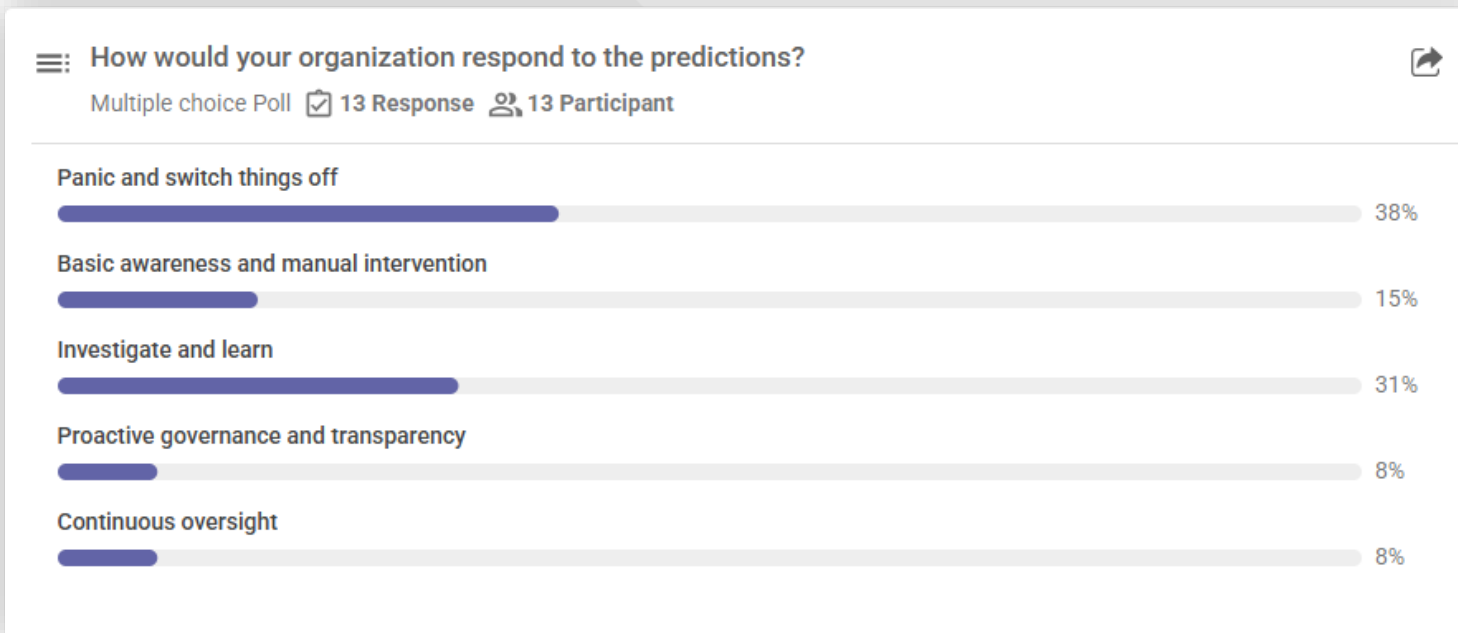
• data leak

What is Governance?

Governance \neq Risk Management

If it was, we should just call it risk management!

The word “**govern**” means “**to steer**”, so it is fundamentally about opportunity realization as well!



To effectively govern you need

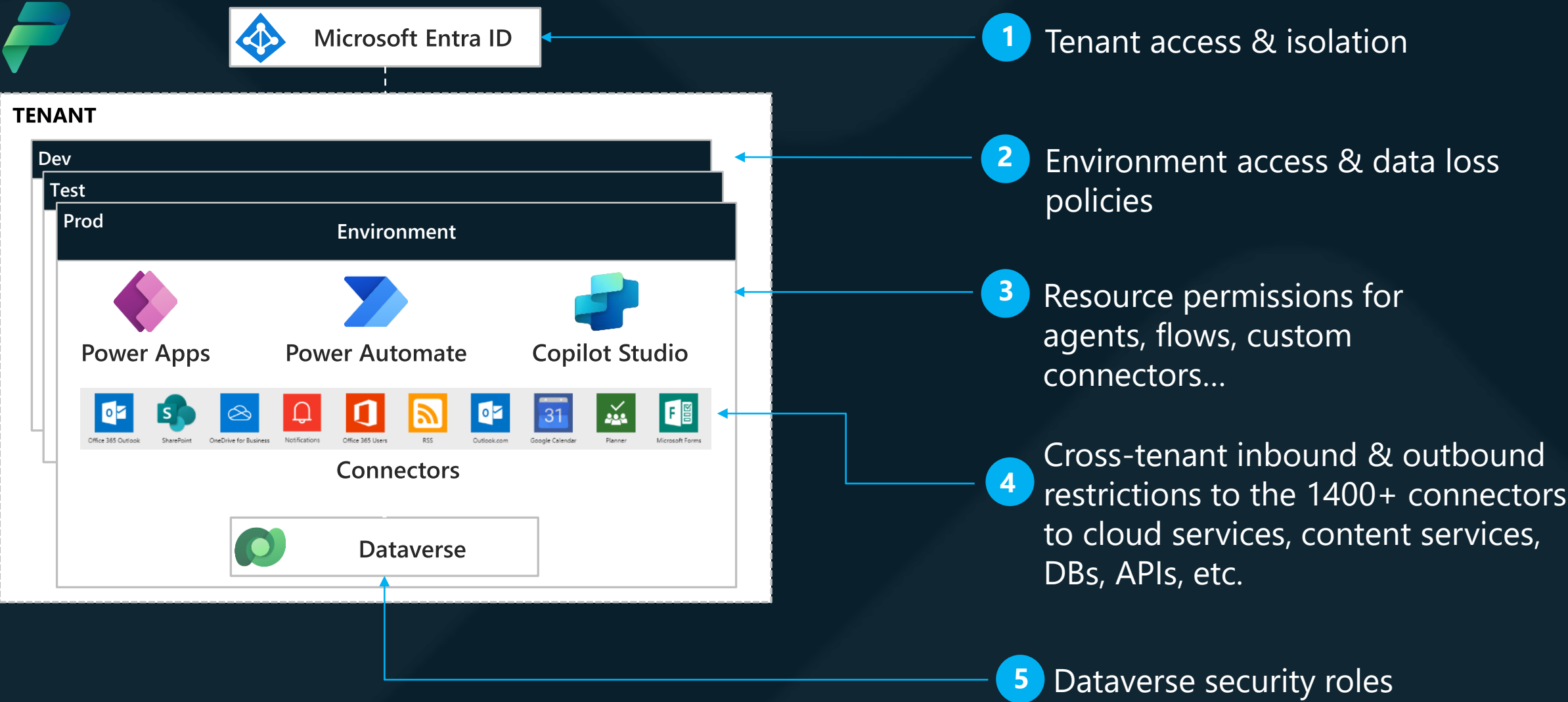
Goal Clarity

Role Clarity

Task Clarity



Governance & Security Overview



Where do you build **agents** in your organization today?



Poll

Poll link: aka.ms/AiWebinars/Polling

Passcode: PowerCAT





How Can I boost innovation and productivity while controlling risks and costs in an era of Gen AI?



How can I protect AI resources and data?



How can I drive cost efficiency and ROI?



How can I place guardrails in place at enterprise scale?



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 communicate and help drive healthy adoption?



Zoned Governance Framework


Governing agents by segmenting by audience + exposure and complexity + risk into zones.



Safe Innovation Zone (Green)
Self-service “sweet spot” for rapid AI agent experimentation with minimal oversight



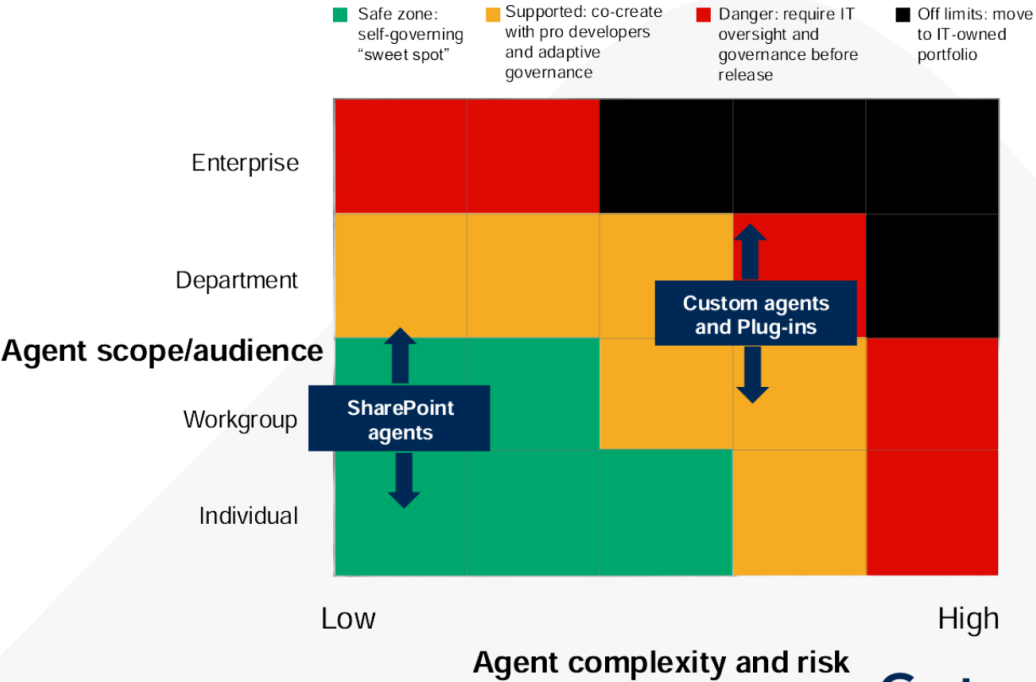
Collaboration Zone (Yellow)
Medium-risk scenarios (Department-level). Requires some admin governance



Enterprise Zone (Red, Black)
High-risk, mission critical scenarios. Demands strict IT/Management control

EXPOSURE	EXTERNAL FACING	SCALE & COMPLEXITY	CRITICALITY		UNDERLYING DESIGN RISKS
	External (Customer - B2C)	High: Global use across Shell, multiple data sources, complex system integration	SOX/KNS (by authorized capability centers)	Business Critical	
	External (B2B, supplier, partner, etc.)	Medium: Business/Function use, some data sources with some system integration			
	Internal	Low: Me/my team, available data sources with simple integration			
Using Approved DIY Platforms / No Duplicating IDT Solutions		CONFIDENTIALITY LEVEL & DATA TYPES		Unrestricted, Restricted and Confidential (Business related only)	Confidential (Legal & Regulatory incl. Sensitive Personal Data)
		IDENTITY MANAGEMENT, AUTOMATION & HIGH PRIVILEGED ACCESS		Using your own Shell ID	Using functional accounts for transactional work
		[OPEN-SOURCE] CODE			Using functional accounts with high privileged system access
					Using Shell approved tools, methods & practice

Source: Forrester Research, Inc.



Why the Safe Innovation Zone Matters

1. **Empower Makers:** Quick creation of low-risk agents with minimal friction
2. **Scale Innovation:** Identify the high value scenarios emerging from early experiments that are growing in adoption
3. **Admin Efficiency:** Safeguards must be in place so admins can dedicate effort where risk is higher

Today, *Default Environment and Developer Environment* empower Makers to get started, but it requires Admin setup to ensure safeguards are in place. Without them, all environments behave like the "Yellow Zone"



DEFAULT ENV

Shared Environment for everyone in the Company

Allows for low risk Agents, flows, Apps to be shared with others in the company



DEVELOPER ENV

Personal environment per Maker

Allows for Makers to build personal agents, flows, apps with richer functionality



OTHER ENVs

Trial, Sandbox, Production

Allows Makers who can create or acquire other environments full access to create custom agents, apps, flows

COLLABORATION ZONE (YELLOW ZONE) IF NO SAFEGAURDS ARE IN PLACE



Proposal: Default configuration for Safe Innovation Zone



DEFAULT ENV

Agents grounded in M365 data with no external actions.

Allowed: MSFT Enterprise plan & Power platform core connectors

Blocked by Default: Other connectors

Sharing: Available to everyone in Env

Agent Settings:

User Authentication Required

Run As: End user context only

No Autonomous Agents

Custom skills blocked

Channels: M365, Teams



DEVELOPER ENV

Agents with actions and autonomous agents. Limited to Maker only usage

Allowed: All Connectors

Blocked by default: None

Sharing: Available only to Maker

Agent Settings:

User Authentication Required

Run As: End user context only

Autonomous Agents allowed

Custom skills blocked

Channels: M365



OTHER ENVs

Full Custom Agents capability but with Admin approvals as needed

Allowed: All Connectors

Blocked by default: None

Sharing: No limits

Agent Settings:

User Authentication Required

Run As: End user context by default

Autonomous Agents allowed

Custom Skills allowed

Channels: All

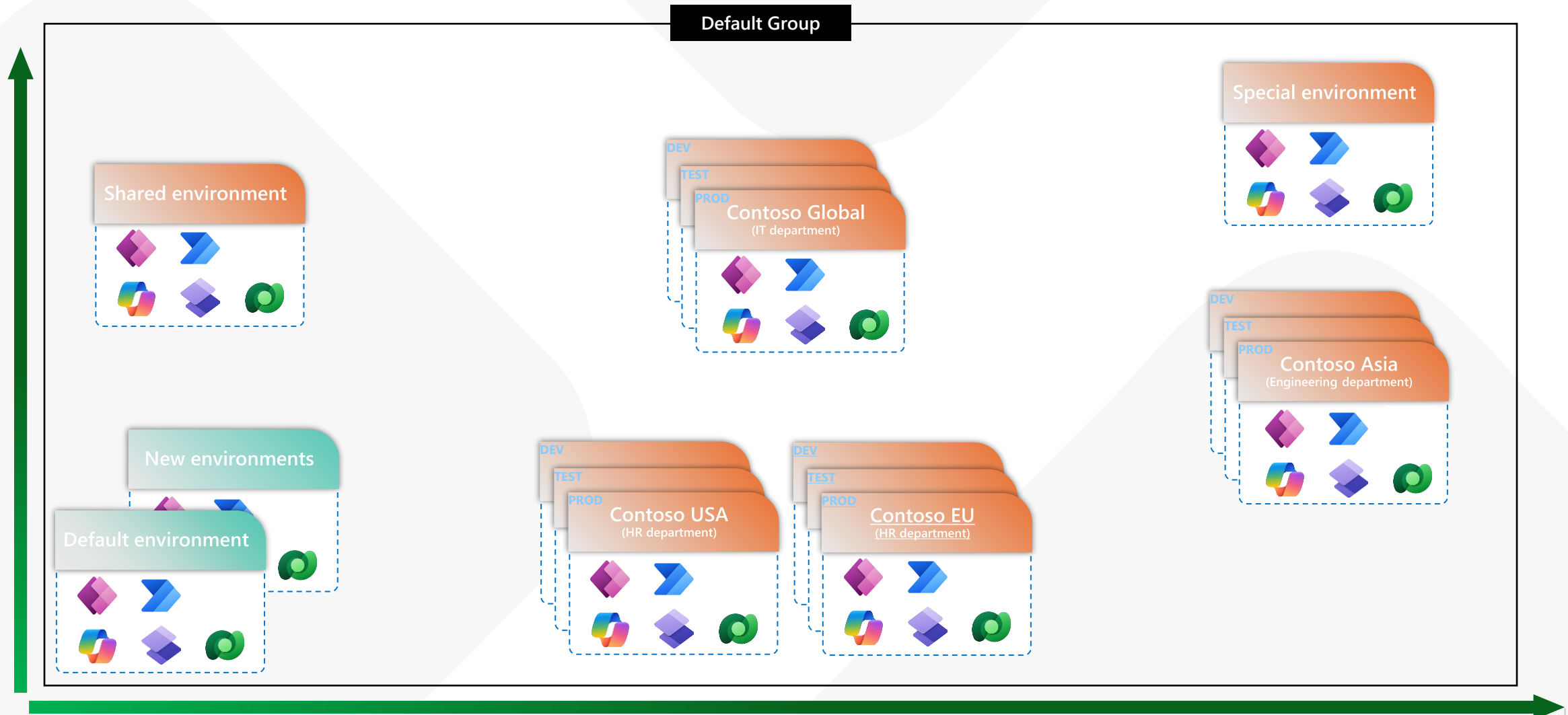
SAFE INNOVATION ZONE (GREEN ZONE)

COLLABORATION ZONE (YELLOW ZONE)



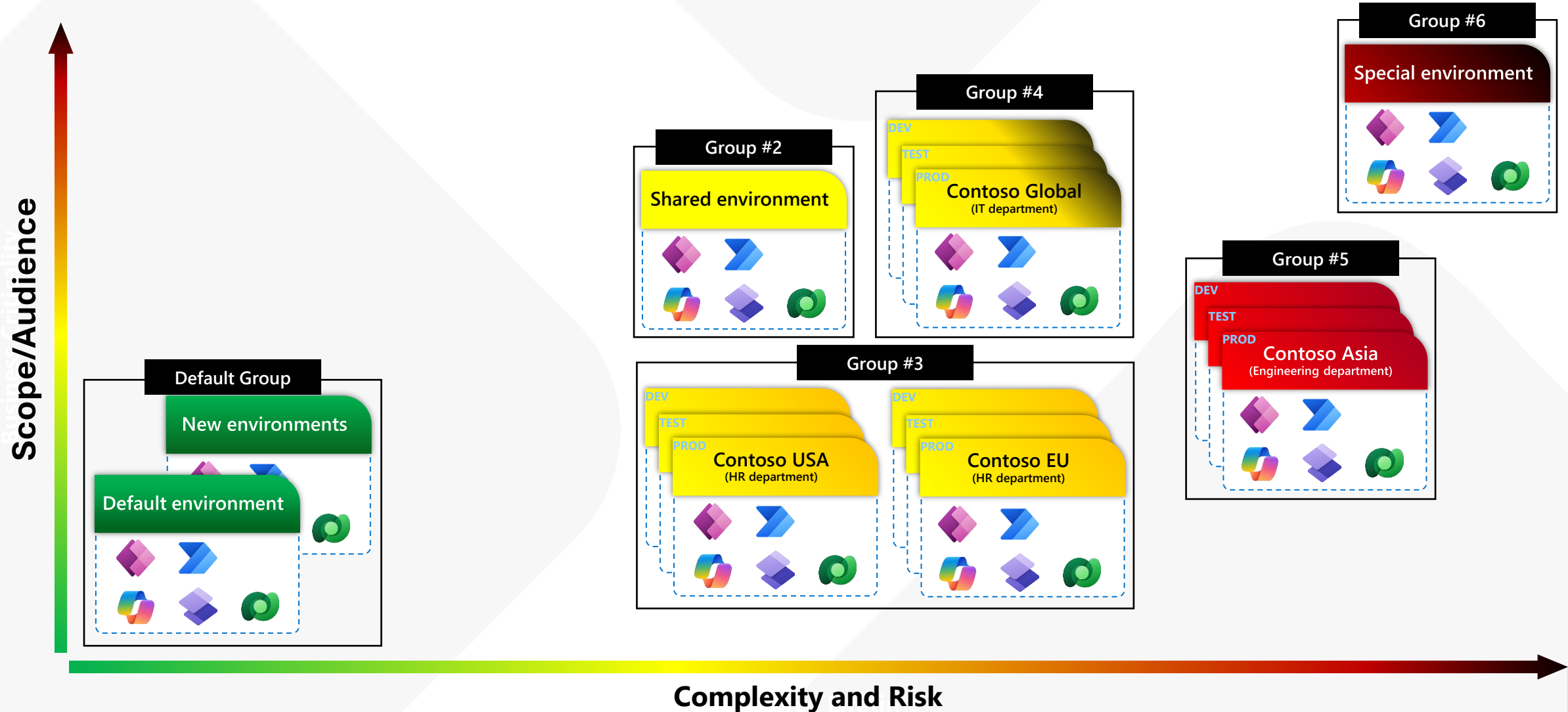
Empowerment through Zoned Governance

An example of an empowered, yet fully governed approach



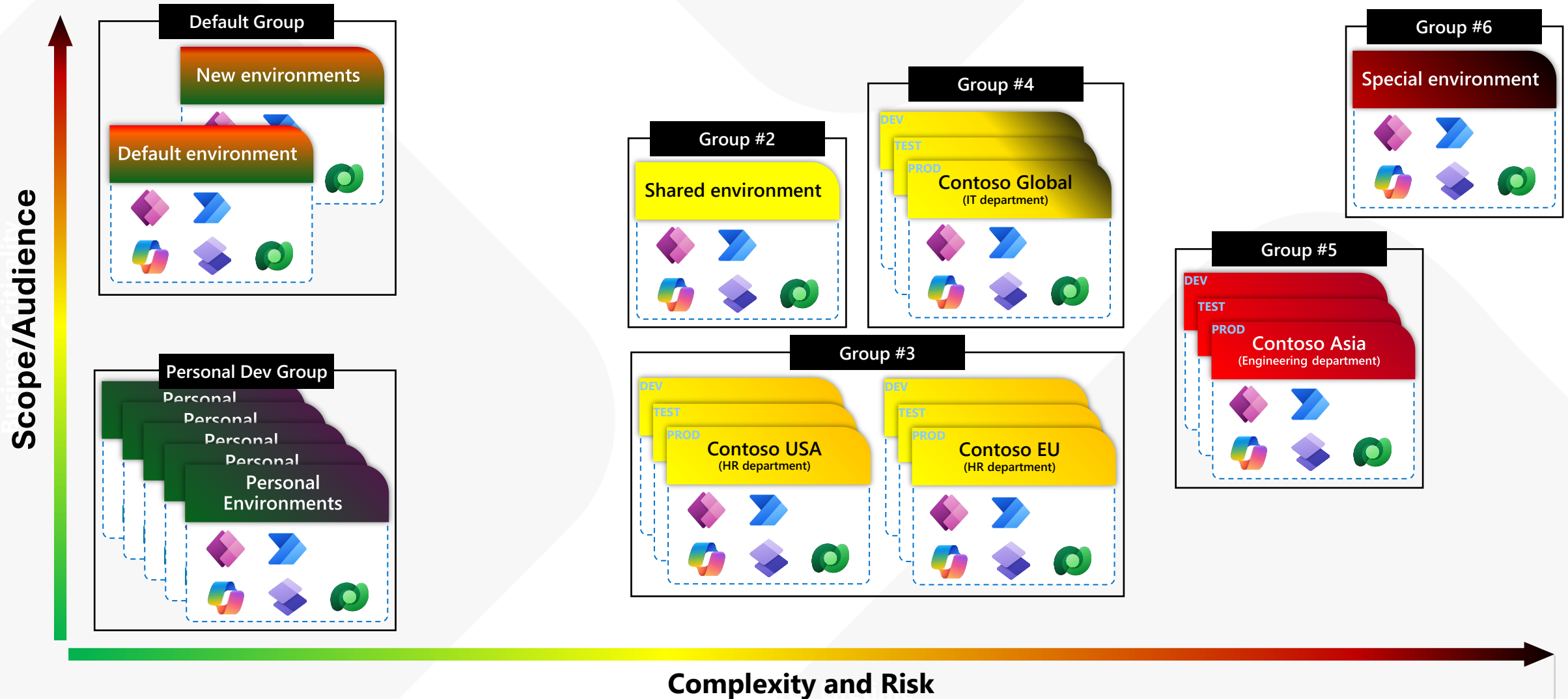
Empowerment through Zoned Governance

An example of an empowered, yet fully governed approach



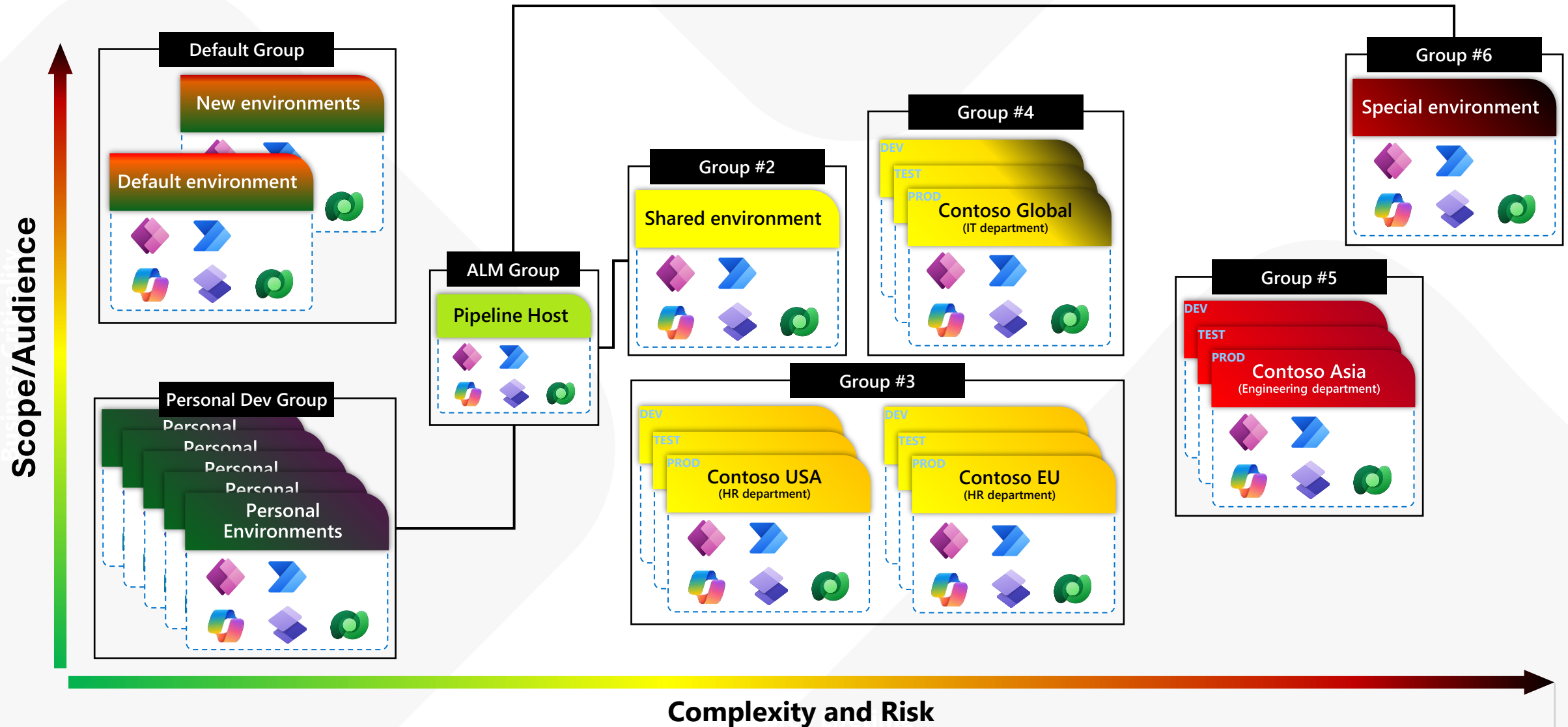
Empowerment through Zoned Governance

An example of an empowered, yet fully governed approach



Empowerment through Zoned Governance

An example of an empowered, yet fully governed approach



Power Platform Admin Center Demo



A developer working on the agent inadvertently configures the agent to read knowledge from a sensitive source.



How do you currently secure and manage data in your organization?



Poll

Poll link: aka.ms/AiWebinars/Polling

Passcode: PowerCAT



Connector Policies – Prevent data exfiltration



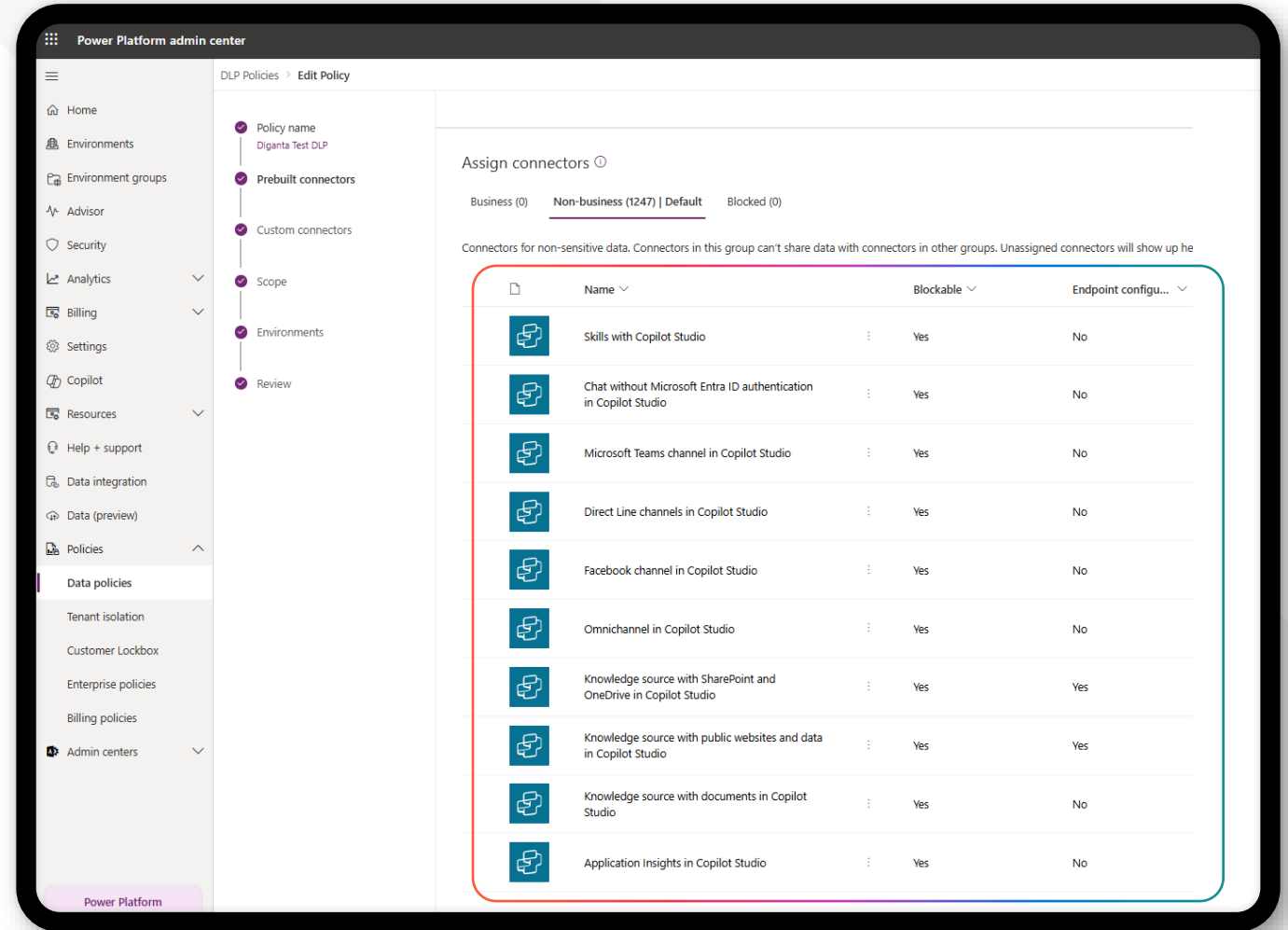
Secure agent by disabling publish



Secure agent by disabling access from internet to chat



Govern agent knowledge and actions connectors using policy



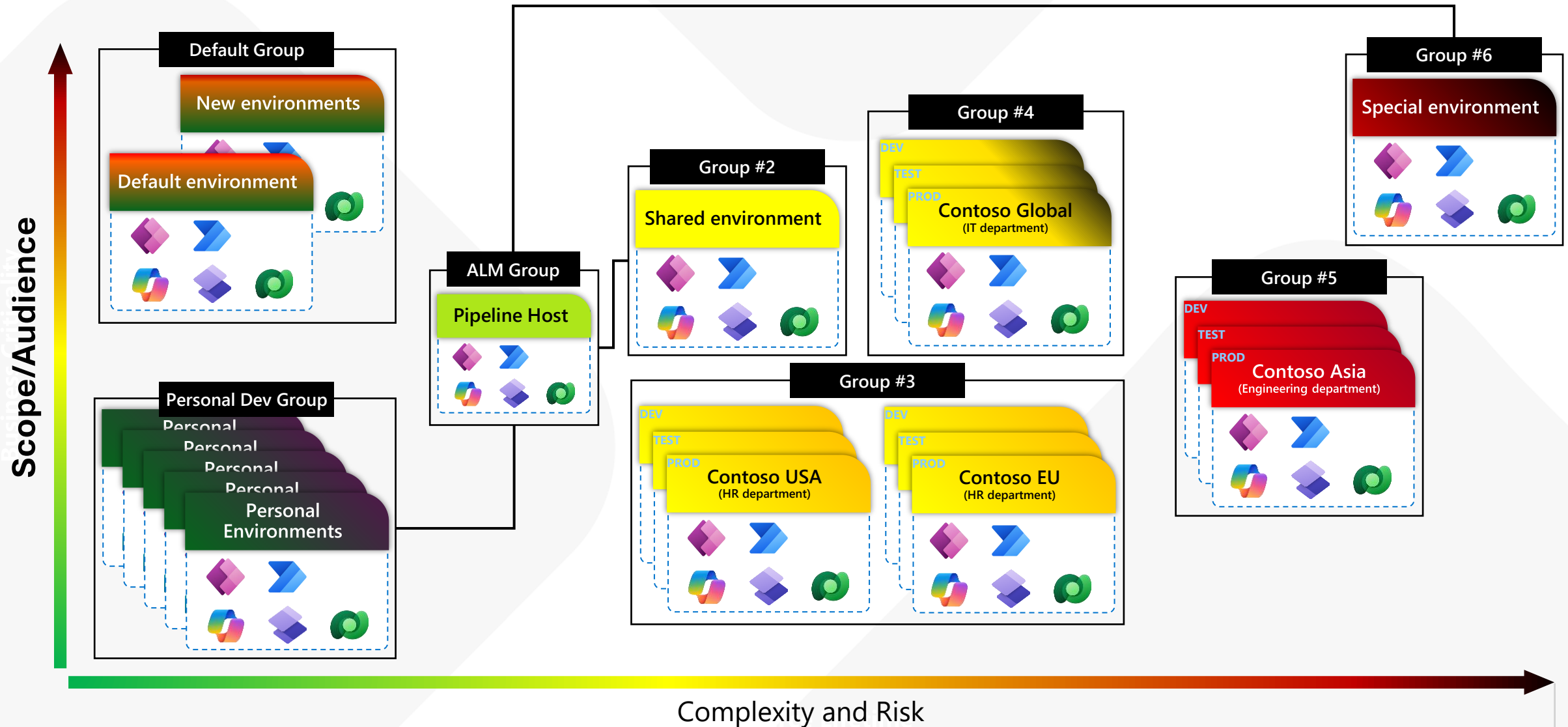
Connector Policies Demo



Empowerment through Zoned Governance

An example of an empowered, yet fully governed approach

aka.ms/environmentstrategy



Focusing Admin Oversight WHERE IT counts

Manage higher risk zones

Safe Innovation Zone: Safe defaults reduce continuous monitoring. Admins can be hands off

Collaboration/Enterprise Zone: Focus your governance efforts (approvals, DLP, Tighter policies) on Dept level and Enterprise critical agents

Strengthen oversight & lifecycle management

Inventory & Audits: Keep reviewing agents inventory in Power Platform Admin Center.

Retirement of obsolete Agents: Proactively remove or archive to manage costs and remove clutter

Refine Continuously

Adapt based on usage: As agent adoption grows, revisit environment policies and connector classifications

Educate & Empower: Provide training and best practices so makers can stay aligned with organizational rules

RESULT

Innovation at Scale

Reduced Risk

Cost & Compliance Management





Secure

MANAGED SECURITY

Advanced protection for an AI-driven world

Security posture management

Threat protection

Data protection and privacy

Identity and access management

Compliance

CIO



Govern

MANAGED GOVERNANCE

More visibility, More Control,
Less effort

Management at scale

Environment strategy

Reactive governance

Full visibility

Capacity and cost management



Operate

MANAGED OPERATIONS

Operational excellence for mission
critical applications

App lifecycle management

Observability

Data Resilience

Quality checker

Test automation

A fully managed platform to enable scale and reduce risk





MANAGED SECURITY

Advanced protection for an AI-driven world

Security posture management

Threat protection

Data protection and privacy

Identity and access management

Compliance



MANAGED GOVERNANCE

More visibility, More Control,
Less effort

Management at scale

Environment strategy

Reactive governance

Full visibility

Capacity and cost management



MANAGED OPERATIONS

Operational excellence for agents
at scale

App lifecycle management

Observability

Data Retention and Mobility

Quality checker

Test automation



INTRODUCING

MANAGED AVAILABILITY

Enterprise Grade Reliability and
Availability for Mission Critical
Workloads

Hyper Availability (Az)

BCDR Agility

A fully managed platform to enable scale and reduce risk





Security hub

Enables AI-powered enterprise-ready security management at scale by providing comprehensive security and global compliance

SIMPLIFY

'Single pane of glass' to help customers discover and secure

Proactive rules to minimize security risks

Timely security recommendations and alerts to effectively react to threats

PROTECT

Tailored recommendations to all asset types

Easy to secure at enterprise scale

Visibility across the entire tenant

Help Makers build securely, and catch problems before they grow bigger

OPINIONATED

Intuitive self assessment experiences

Strategic guidance that can be personalized

Safe and secure defaults

Help customers prioritize actions based on the level of security risks

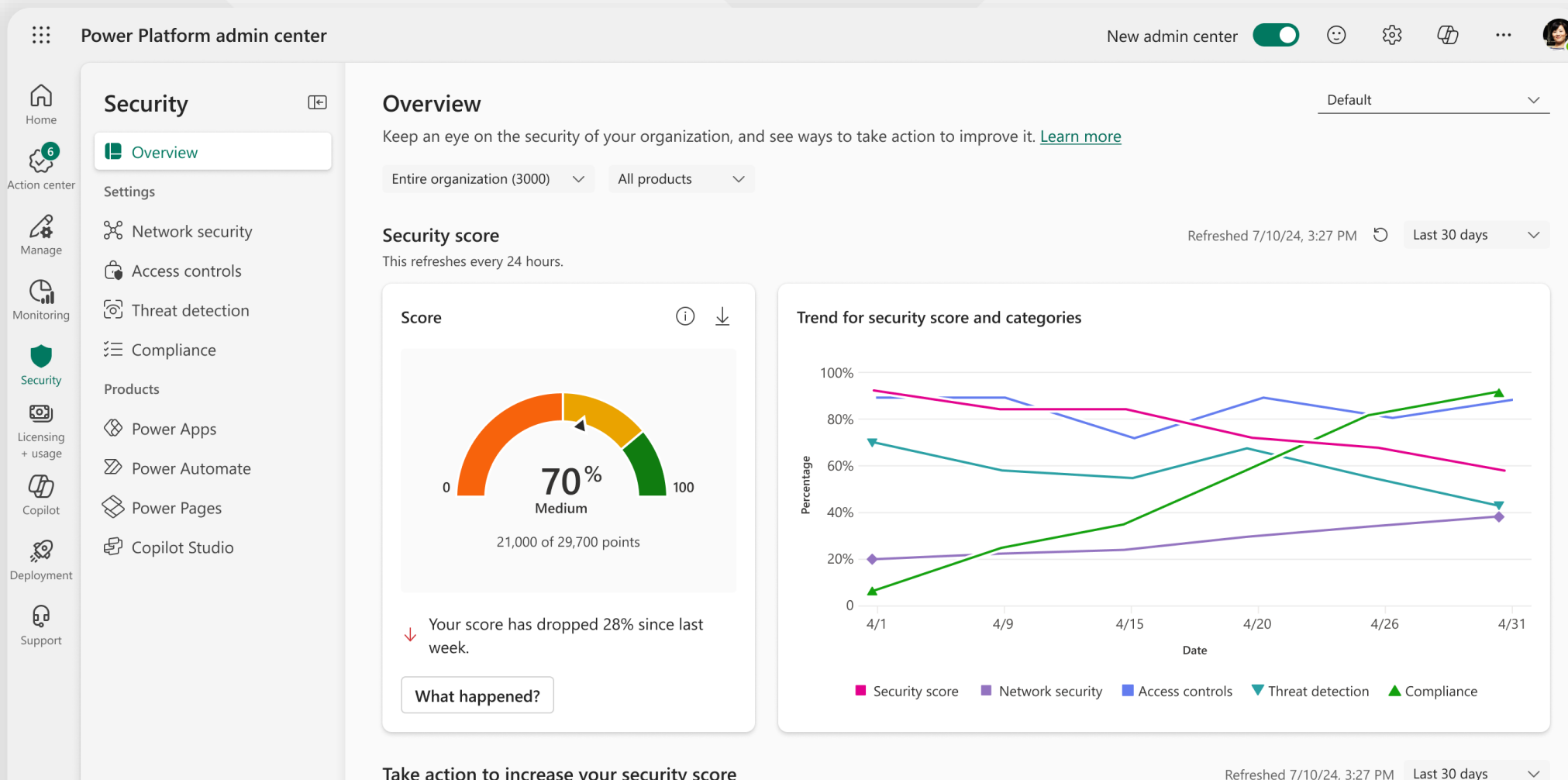
aka.ms/PPAC/SecurityPage





Security hub

Enables AI-powered enterprise security management at scale



Managed Security

Advanced protection for an AI-driven world

Security Posture Management

Intelligent guidance for scalable and efficient enterprise-grade security.

Security guidance

Data Protection and Privacy

Robust controls to ensure confidentiality and encryption, ensuring security of sensitive information.

Customer managed keys

Data masking

Microsoft Purview Data map integration

Data policies

Network Isolation (v-Net)

Identity and Access Management

Seamless and adaptive tools to ensure only authorized resource and data access.

IP Firewall

Resource sharing limits

IP cookie binding

Privileged Access management

Resource sharing limits

Authentication controls

Compliance

Assured visibility and adherence to industry and regional regulatory requirements.

Lockbox

Dataverse audit

Threat Protection

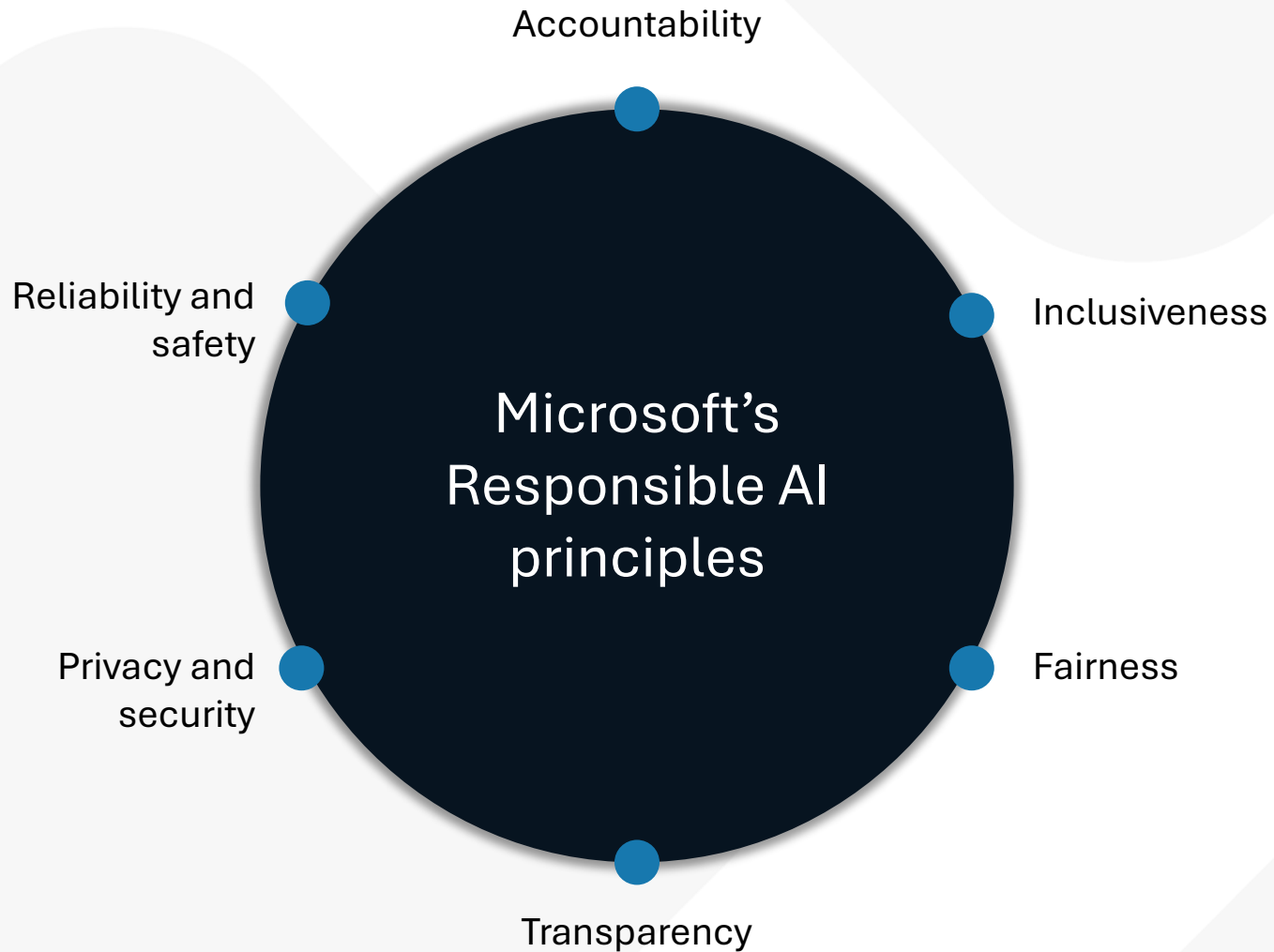
AI-powered detection and monitoring to address and prevent security risks.

Enforceable solution checker

Microsoft Sentinel integration



Microsoft's Responsible AI Principles



Building blocks to enact principles



Tools and processes



Training and practices



Rules



Governance

aka.ms/AiRisks



Governance and Security Controls for Your **Copilot Studio** Agents



Security

Security controls for agent knowledge and actions

Set policies and information labels to discover, classify, and protect sensitive data

Streamline security effectiveness and gain visibility of security posture



Adoption

Enforce application Lifecycle management best practices

Standardize assets and maintain design patterns

Capture interactions with auditing and compliance monitoring



Monitor and Control

Build, deploy, and enforce environment governance strategies

Gain visibility of agent usage in Power Platform and grow adoption

Proactive governance with actionable recommendations to govern, manage, and secure your low-code assets



What are the **3 key things** your organization would do in next three months?



Poll

Poll link: aka.ms/AiWebinars/Polling

Passcode: PowerCAT



Before we get to Q&A, please provide your feedback

aka.ms/AIGov/Feedback



Ready for more?



→ **April 29th (EMEA)** : Unlocking the Potential of Copilot Studio
(6 a.m. PST / 1 p.m. GMT)

April 30th : Data foundations for AI

May 7th : Application Lifecycle Management

aka.ms/powercat/aiwebinars



Get started today



aka.ms/trycopilotstudio



Learn more

Copilot Studio website: [aka.ms/**copilotstudio**](https://aka.ms/copilotstudio)

Blog: aka.ms/copilotstudioblog

Public Demo: [aka.ms/**copilotstudiodemo**](https://aka.ms/copilotstudiodemo)

Learn Docs: [aka.ms/**copilotstudiodocs**](https://aka.ms/copilotstudiodocs)

Community page: [aka.ms/**copilotstudiocommunity**](https://aka.ms/copilotstudiocommunity)

Copilot Studio Resources: aka.ms/copilotstudio/resources

Copilot Studio
Implementation Guide: [aka.ms/CopilotStudio/Implementa
tionGuide](https://aka.ms/CopilotStudio/ImplementationGuide)



Q&A!

aka.ms/AIWebinars/Questions

☰ Respond | Power CAT AI Webinars: Intro

🌙

👤

Q&A

POLLS

🔍 Search questions

Ask anonymously

😊 | ➤

Popular

Recent

#Questions: 0

Please ask your question!

There is no active question yet

Thank you for participating!

