Responsible AI and Copilot Readiness With Microsoft Purview

SOLID AI — Microsoft HQ Redmond

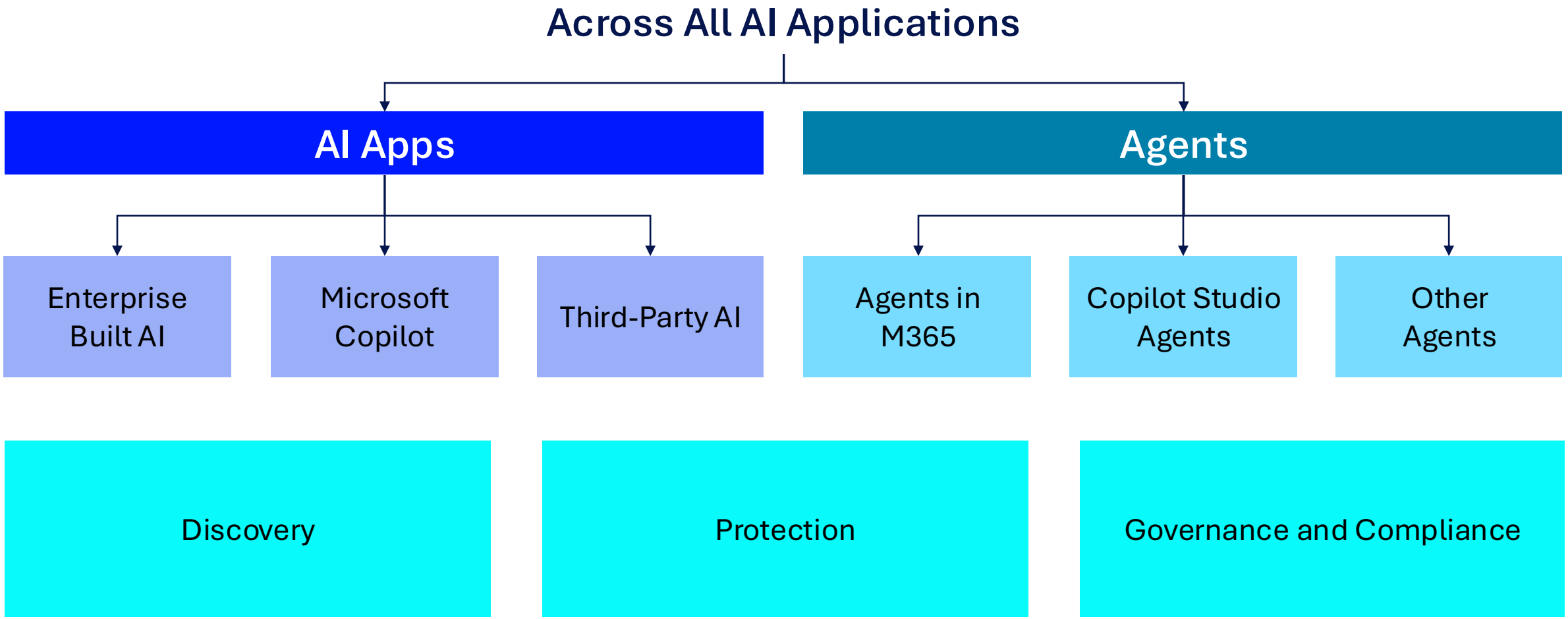
Shilpa Ranganathan, Principal Group PM, Microsoft Purview

Jon Kessler, Vice President and General Manager, IG - Legal Solutions

August 7, 2025

Microsoft Purview

Comprehensive solution to secure and govern AI.



AI Transformation With Copilot Is Happening Now

75%

of knowledge workers already using AI at work (doubled in the past 6 months).[1]

30min

saved a day, equating to 10 hours per month by Copilot users.[2]

65%

of organizations using and deriving business value from gen AI in 2024.[3]

$3.5

return on investment for every US$1 invested into AI.[4]

1. Work Trends Index
2. Work Trends Index
3. McKinsey
4. IDC

Top Security and Compliance Concerns With AI Usage

1

Data Oversharing

Users may access sensitive data with AI apps they're not authorized to view or edit.

2

Data Leak

Users may inadvertently leak sensitive data to AI apps.

3

Risky Usage

Users leverage AI apps to generate unethical or other high-risk content.

Real World Impacts of AI Adoption with No Responsible AI Program

High Tech Internal Code Leak

Employees used personal ChatGPT accounts to debug code and summarize internal documents, inadvertently leaking their source code and internal data.

Retail IP Leak

Employees uploaded confidential information to ChatGPT, which the model then trained on. They noticed this only when responses from ChatGPT closely resembled sensitive company information.

Widespread Data Breaches

Cybernews analyzed 52 popular AI tools, 84% had experienced data breaches of IP, PII, and credentials. Most tools lacked enterprise-grade security, causing AI integrations to act as data exfiltration points of failure.

Exposing Trade Secrets to ChatGPT

A Fast Company Report found that 14% of AI users admitted to entering company trade secrets into ChatGPT, often using personal accounts outside the scope of corporate monitoring systems.

Source: Forbes, Prompt Security, Fast Company

How Do I Think Holistically About the Many Challenges of AI Adoption?

Organizations face several people, process, and technology-related hurdles with AI implementations.

People

- **Lack of training** on department-specific **use cases.**
- Users **sharing sensitive information** with unsanctioned **public AI** solutions.
- Frustrations with **poor results** leading to **decreased adoption.**
- **Increased risk of data leakage** after deploying AI tools without proactive controls around sharing and access.

Process and Technology

- **Undefined policies and procedures** for governance, retention, and discovery of AI prompts.
- **Poor data quality management** leading to inaccurate or unreliable AI model outputs.
- **Absence of a central oversight body** to oversee AI usage, set goals, and ensure compliance with best practices.
- **Lack of clarity** around available **controls** to protect sensitive content as well as monitor and report on AI usage.

What Does a Responsible AI Journey Look Like?

epiq

Microsoft Compliance Partner of the Year
2022 Finalist
2023 Winner
2024 Finalist

Responsible AI and Copilot Readiness

Expedite time to value while reducing risk, optimizing for AI, and ensuring compliance.

Assessment and Strategy

1 Strategy, Planning, and Design

Review AI readiness across people, processes, and technology. Start building an AI governance program, identify gaps, and agree on an adoption plan.

2 AI Data Risk Assessment

Adjust classifiers to detect sensitive data. Start addressing gaps in data protection. Review AI activity and evaluate permissions to identify potential risks.

Educate

3 Copilot User Prompt Training

Maximize the benefits of your investment in AI with business function training, including prompt training and the proper handling of sensitive data.

Implement Data Protection and Security Controls

4 Data Protection Implementation

Implement AI-enabled information protection labels based on common and business specific classifiers.

5 Data Security Controls Deployment

Safeguard data with proactive data loss prevention and AI enabled insider risk management controls.

Improve Data Quality and Ensure Responsible AI Usage

6 Overexposure Remediation

Minimize over-permissive access to sensitive data with technology and change management processes.

7 Data Lifecycle Optimization

Reduce hallucinations with defensible data minimization. Create a comprehensive data lifecycle strategy for AI generated data.

8 AI Prompt Usage Controls

Monitor AI prompt usage in alignment with corporate AI acceptable use policies.

9 AI Apps and Agents Governance

Develop a strategy for governance on custom AI applications, third party AI applications, and Agents.

10 AI Governance Regulations

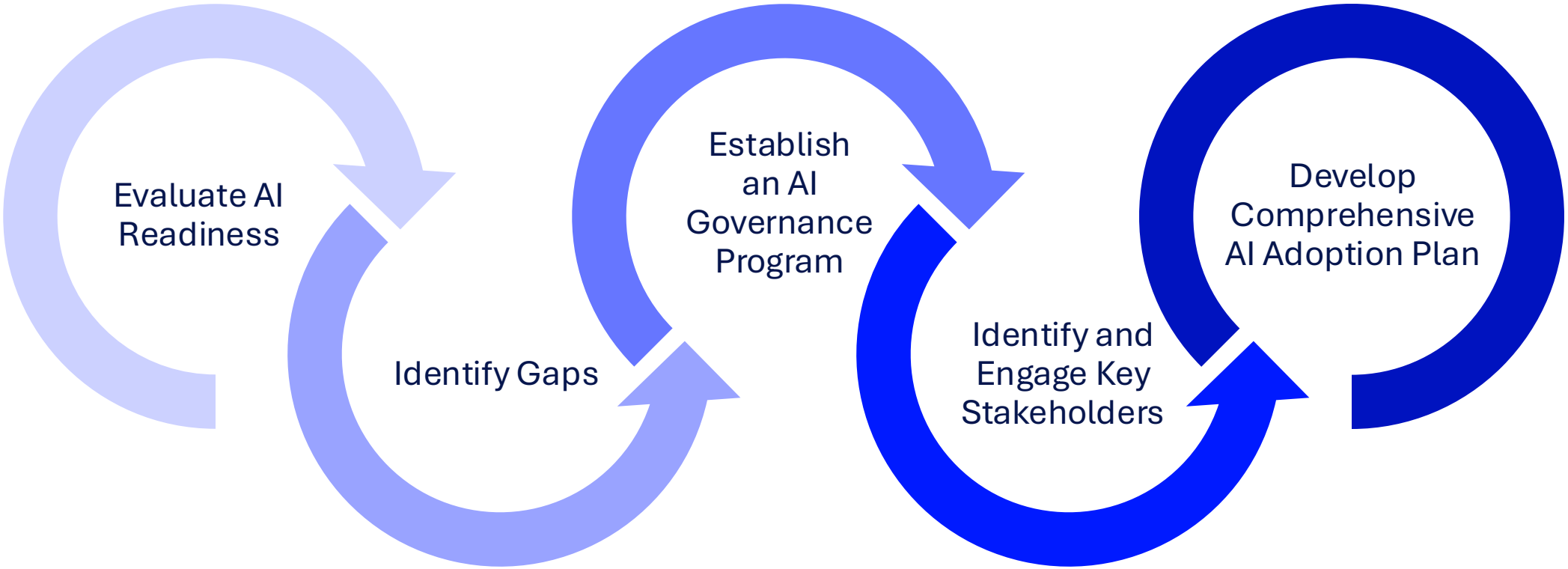
Define and implement processes to comply with evolving global AI governance regulations.

Continuously Reevaluate AI Program and Measure Success

I’d like to begin my AI readiness journey — where do I start?

How Do I Begin My AI Readiness Journey?

Start with a plan and strategy.



How can I get a quick view into my organization’s AI readiness posture?

How Do I Understand the Risk in My Data Environment?

DSPM for AI: Oversharing assessments help identify and classify overshared sites and content and provide recommended actions to mitigate risks.

Identify potentially overshared sites and files

- Sites and files with sensitive data
- Data shared broadly
- Frequently accessed data

Prioritize highest impact risks

- High Risk
- Medium Risk
- Low Risk

Example

A site contains documents with credit card numbers + Everyone in the organization can access the site's content + 575 unique users accessed the site's content last week = **High Risk: Prioritize Remediation**

- Analyze generative AI activity in Microsoft 365 environment.
- Identify patterns in AI usage across different roles and teams.
- Classify sensitive content across SharePoint and Teams.
- Review user access policies and permissions settings.
- Evaluate file permissions to ensure compliance and security.
- Lock down sensitive data locations for enhanced security.
- Integrate DSPM strategies for compliance and risk management.

How can I address the challenges users are facing with adoption of AI chat applications and realize returns on my AI investment?

How Do I Maximize My AI ROI and Get My People up to Speed?

Accelerate AI adoption within your Legal and Compliance team with training to work faster, more accurately, and responsibly.

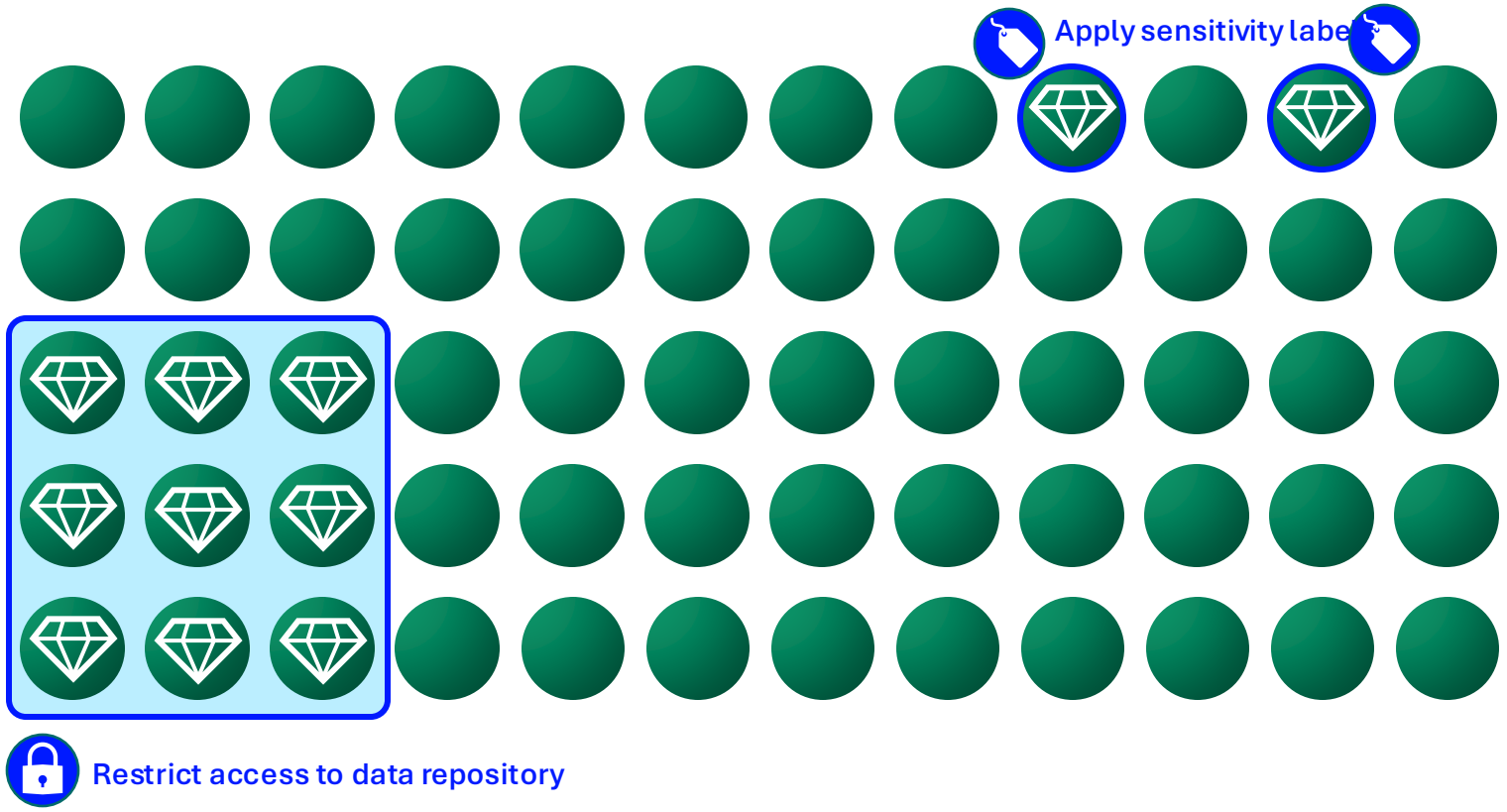
Learn best practices for using Microsoft 365 Copilot and Copilot Agents to:

1. **Understand the fundamentals** of Gen AI Copilots and Agents and how they work.
2. Apply Copilot to **Legal and Compliance use cases**, including document drafting, task automation, regulatory assessment, and other scenarios.
3. Take **full advantage** of Copilot across the entire M365 suite, understanding AI capabilities in each M365 application.
4. Ensure AI tools are **used ethically**, accurately, and compliantly with relevant policies.
5. **Increase productivity** through best practices for basic, multi-step, conditional, and iterative prompt engineering.

How can I find sensitive data in my organization and protect it?

How Can I Ensure My AI Tools Handle Different Data Appropriately?

Microsoft Information Protection (MIP) enables automatic or manual application of sensitive labels that classify data based on sensitivity and these labels guide how AI tools and users should treat the data.

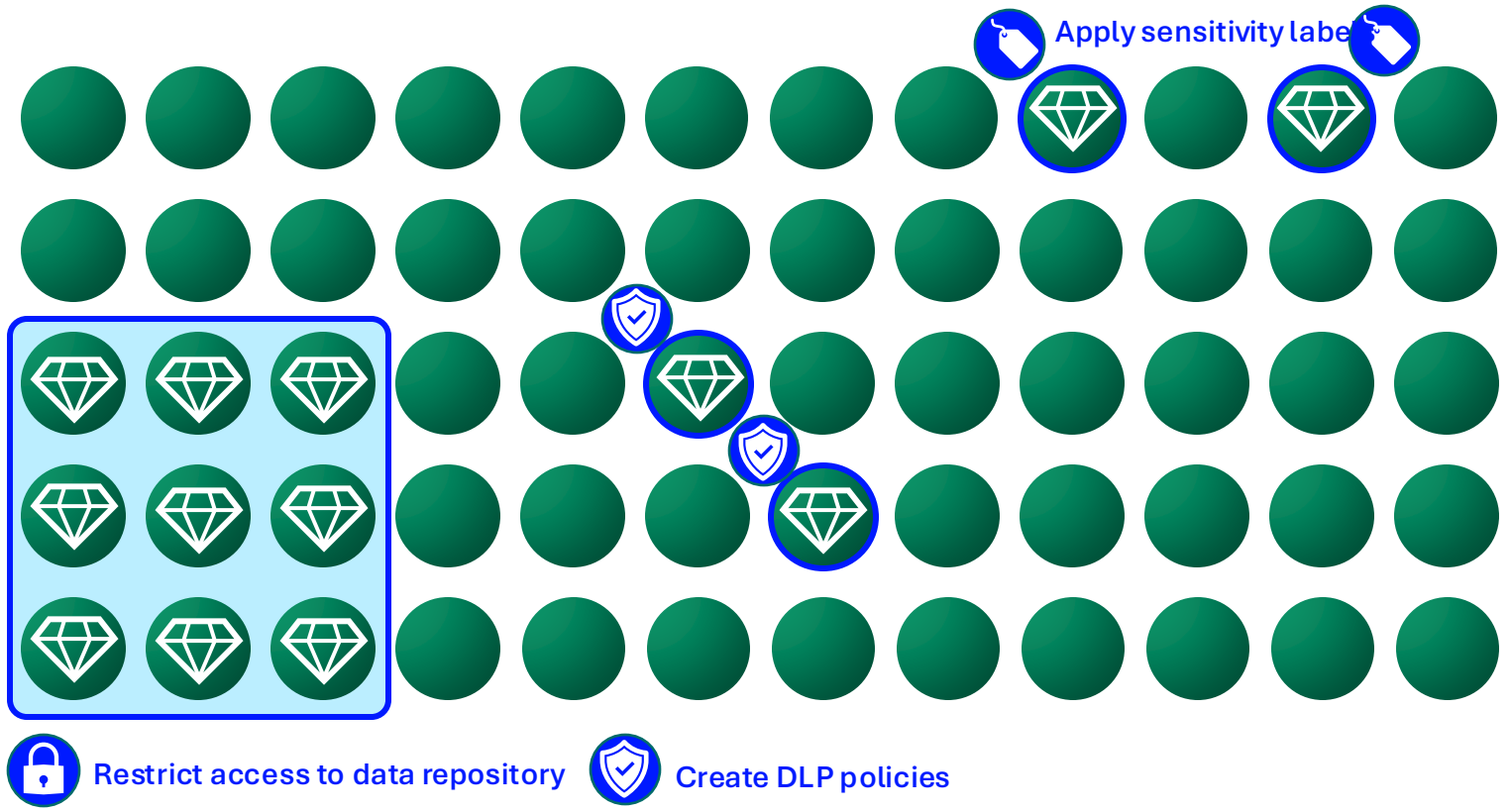


If you prompt anything in Copilot, you won't get anything back from a repository that is classified as restricted.

Can I use proactive controls to protect sensitive data and prevent risky behaviors?

How Can I Prevent Sensitive Data From Being Shared or Leaked by AI?

Insider Risk Management (IRM) and Data Loss Prevention (DLP) prevent data leakage and enforce user controls.

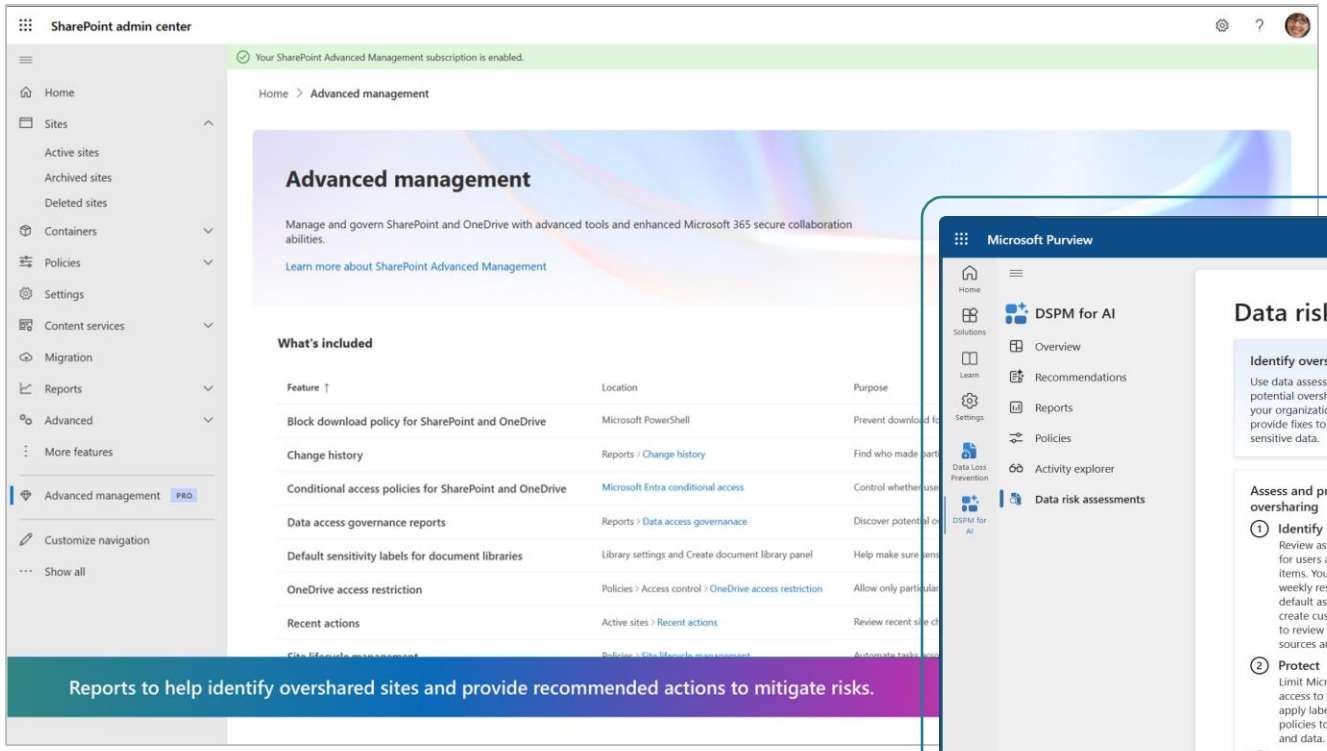


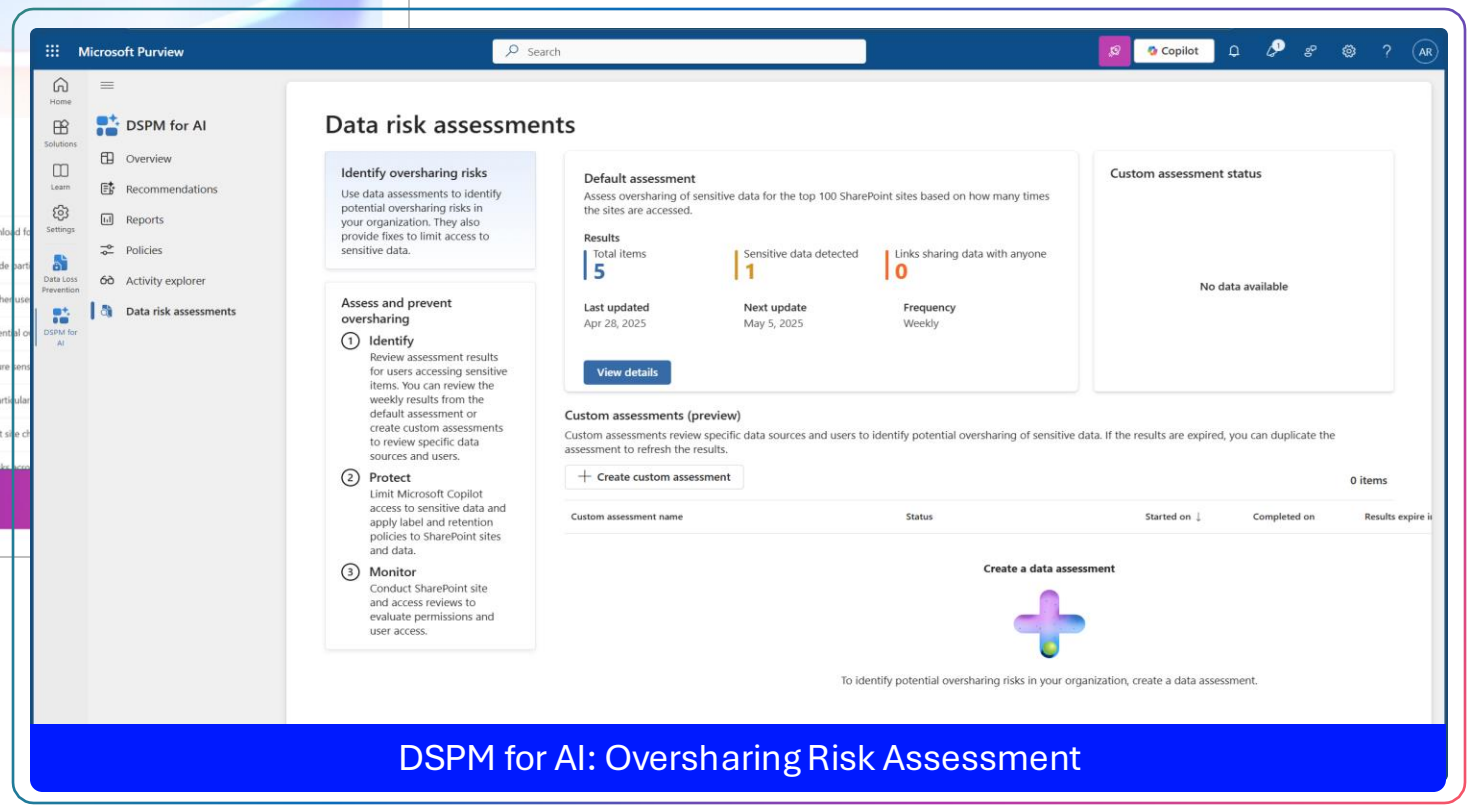
Admins can create IRM policies to detect risky usage based on the classification and sensitivity of the data.

How can I ensure users only have access to the data I expect them to?

How Can I Ensure AI Tools Don't Have Access to Data I Don't Want It To?

SharePoint Advanced Management and DSPM for AI can help you remediate overexposure.





DSPM for AI: Oversharing Risk Assessment

How can I reduce hallucinations and retain AI chat interactions?

How Can I Reduce Hallucinations and Retain AI Interactions?

Microsoft Data Lifecycle Management (DLM) and Records Management (RM) can improve the quality of the data feeding your AI inputs as well as apply retention and disposition to AI interactions.

Redundant	Duplicate files stored across multiple locations
Obsolete	Outdated information no longer needed by the organization
Trivial	Information that provides no value to the organization, such as personal files

Once cleaned up, **Purview Data Lifecycle Management** can prevent ROT accumulation on an ongoing basis.

Better Data Quality = Fewer Hallucinations

Advancements in AI technology will also continue to reduce hallucinations.

Administrators can create new retention policies and apply them to different Copilots.

AI activity data, such as prompts and responses, will be retained inline with the specified policy.

How can I prevent users from using AI chat for nefarious use cases?

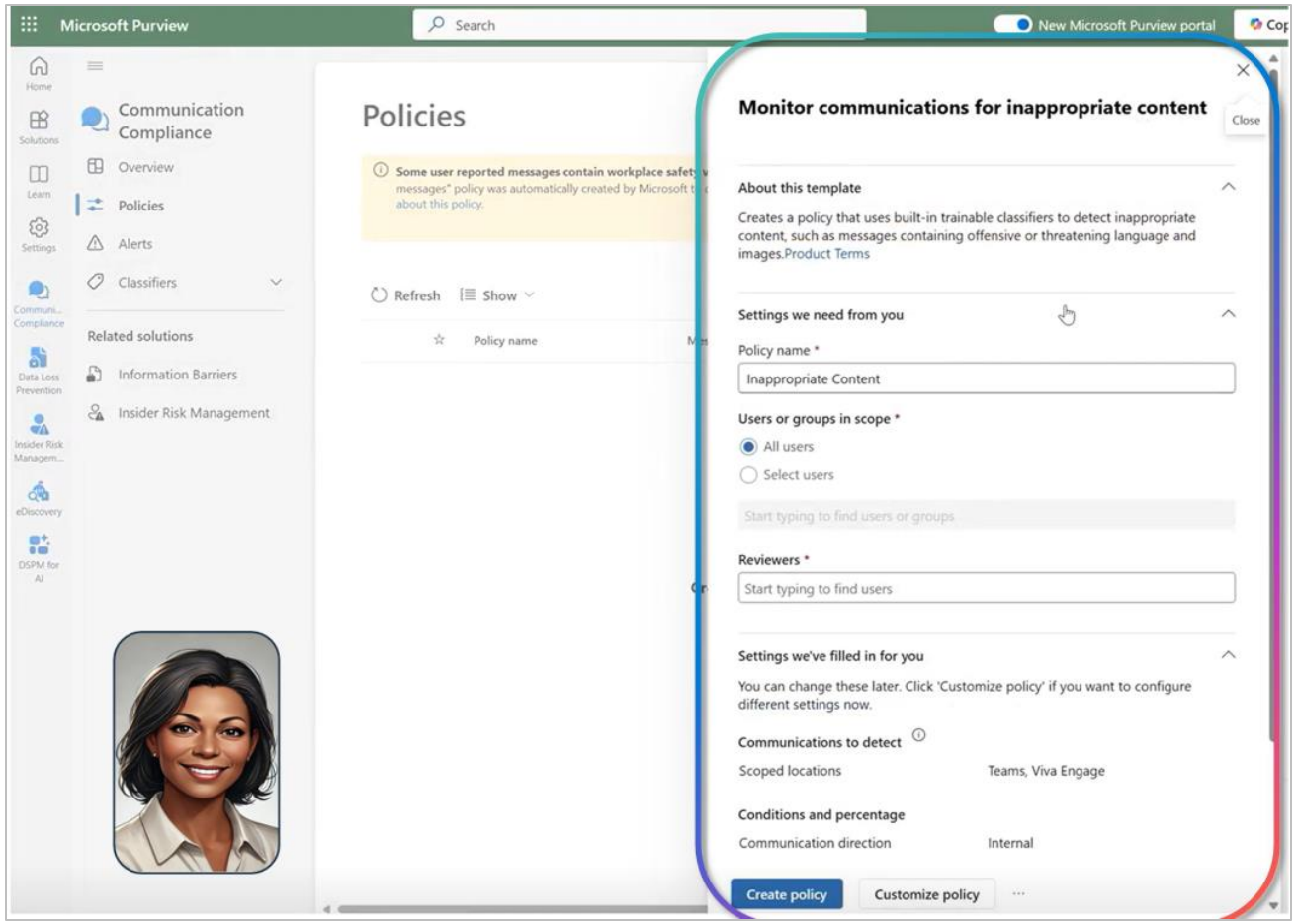
How Do I Monitor How Users Interact With AI Apps?

Communication Compliance (CC) can track and monitor a range of unethical or risky AI behaviors in Microsoft and third-party AI Apps.

CC can detect unapproved, risky, or unethical usage of AI apps
(e.g., harassment, adult content, regulatory violations, sensitive information, etc.).

Admins can create CC policies to detect usage of certain Sensitive Information Types (SITs) within AI apps.

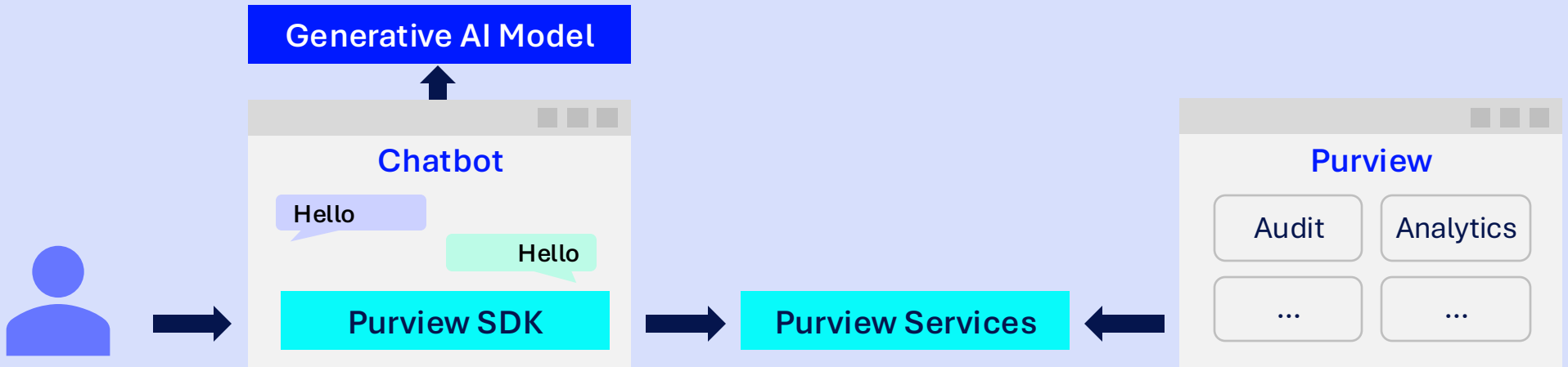
Admins can create IRM policies to detect risky usage based on classification and sensitivity of the data.



How can an organization protect and govern usage of custom and third-party AI apps?

How Do I Govern My Third-Party AI Apps and Custom Copilots?

For a Developer Building Gen AI Solutions:



Agents in Microsoft 365 Copilot

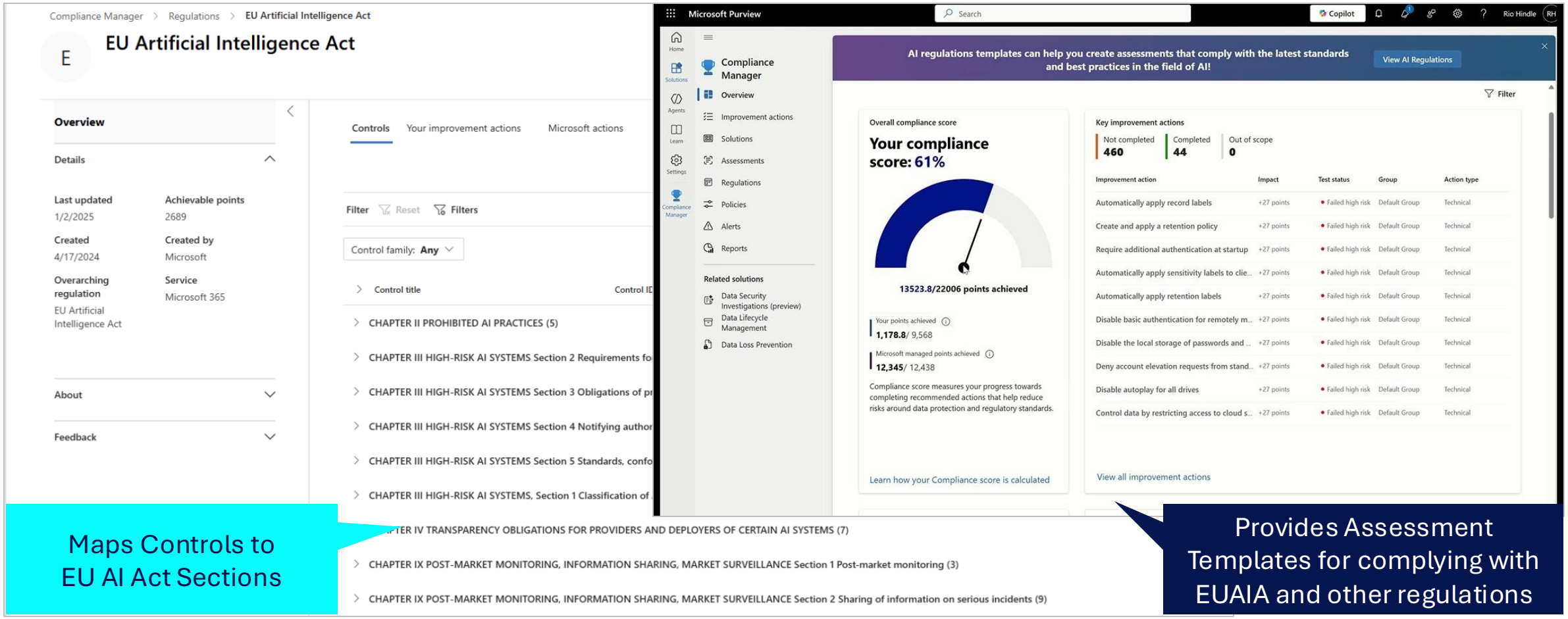
- Microsoft 365 Copilot
- Agent builder
- Copilot Studio
- Meeting facilitator agent
- SharePoint agents
- More M365 agents

Purview policies and protections for Copilot automatically extend to agents.

How can I understand the technical requirements associated with AI regulations and measure my compliance?

How Do I Ensure My AI Tools and Usage Remain Compliant?

Compliance Manager ensures AI tools comply with data residency, content, and retention requirements through capabilities that span assessment, enforcement, and monitoring.



DSPM for AI Live

epiq

Microsoft Purview and Responsible AI

Unified data security, governance, and compliance solutions for all data **and AI apps.**

Discover
Data Risk

Protect
Sensitive Data

Govern
Compliant Usage

Across...

Structured Data + Files and Emails + AI data + M365 and Other Clouds

SOLID AI | Microsoft

Thank you.