



Responsible Copilot Readiness With Microsoft Purview

SOLID AI

Jon Kessler, Epiq

November 2025

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.

Widespread Data Breaches

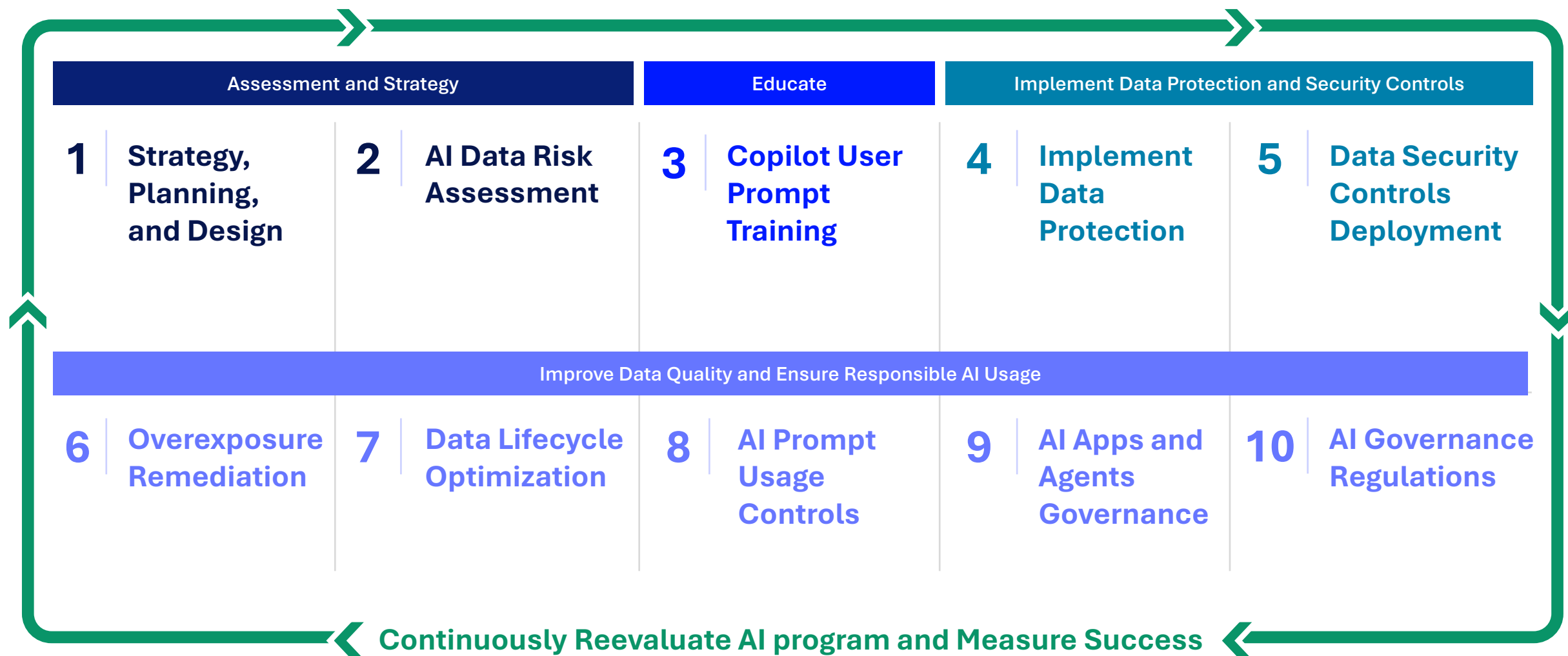
Cybernews analyzed 52 popular AI tools, 84% had experienced data breaches of IP, PII, and credentials.

Exposing Trade Secrets to ChatGPT

A Fast Company Report found that 14% of AI users admitted to entering company trade secrets into ChatGPT.

Responsible AI and Copilot Readiness

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



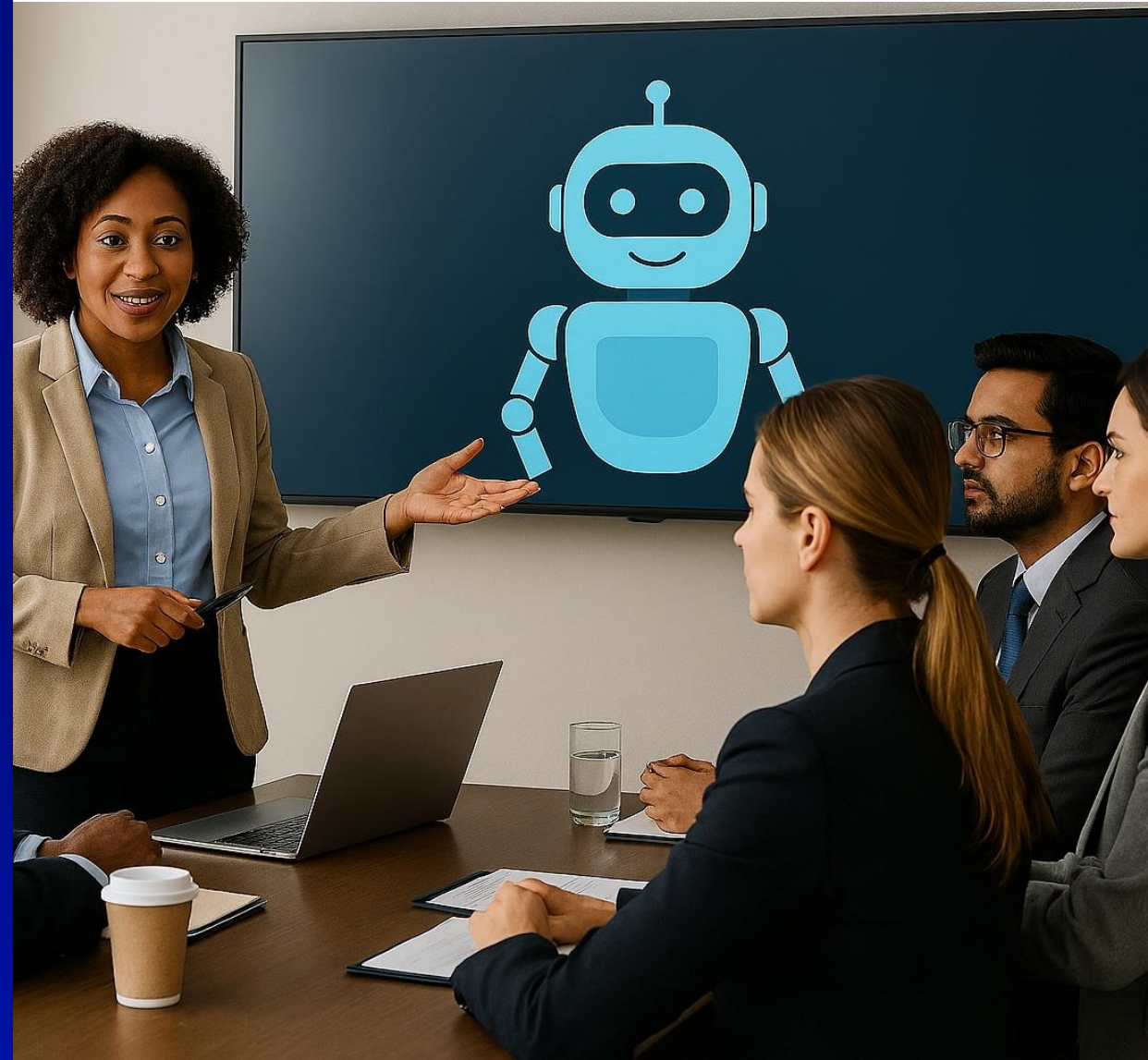
How do I begin my AI readiness journey?



How do I
understand the
risk in my data
environment?



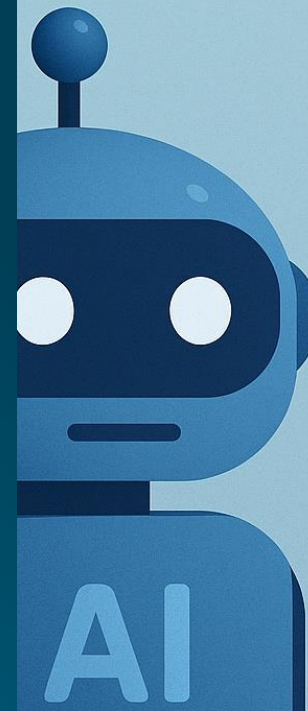
How do I maximize my AI ROI with my workforce?



How can I
ensure my
AI tools
handle data
appropriately?



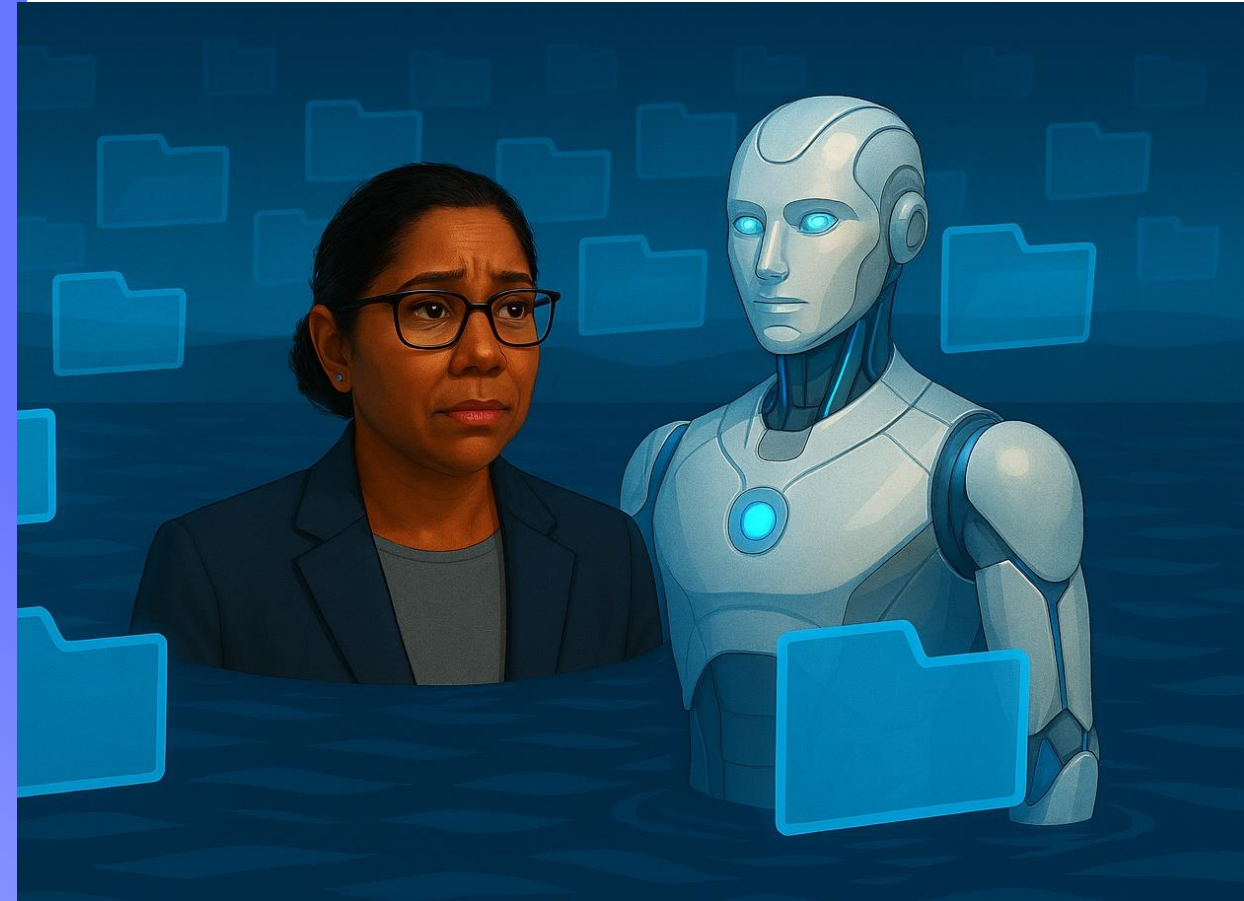
How can I
prevent AI
from sharing
sensitive data?





SharePoint Advanced
Management and DSPM
for AI

How can I
ensure AI tools
don't have
access to all
data?



How can I reduce AI hallucinations and retain AI interactions?

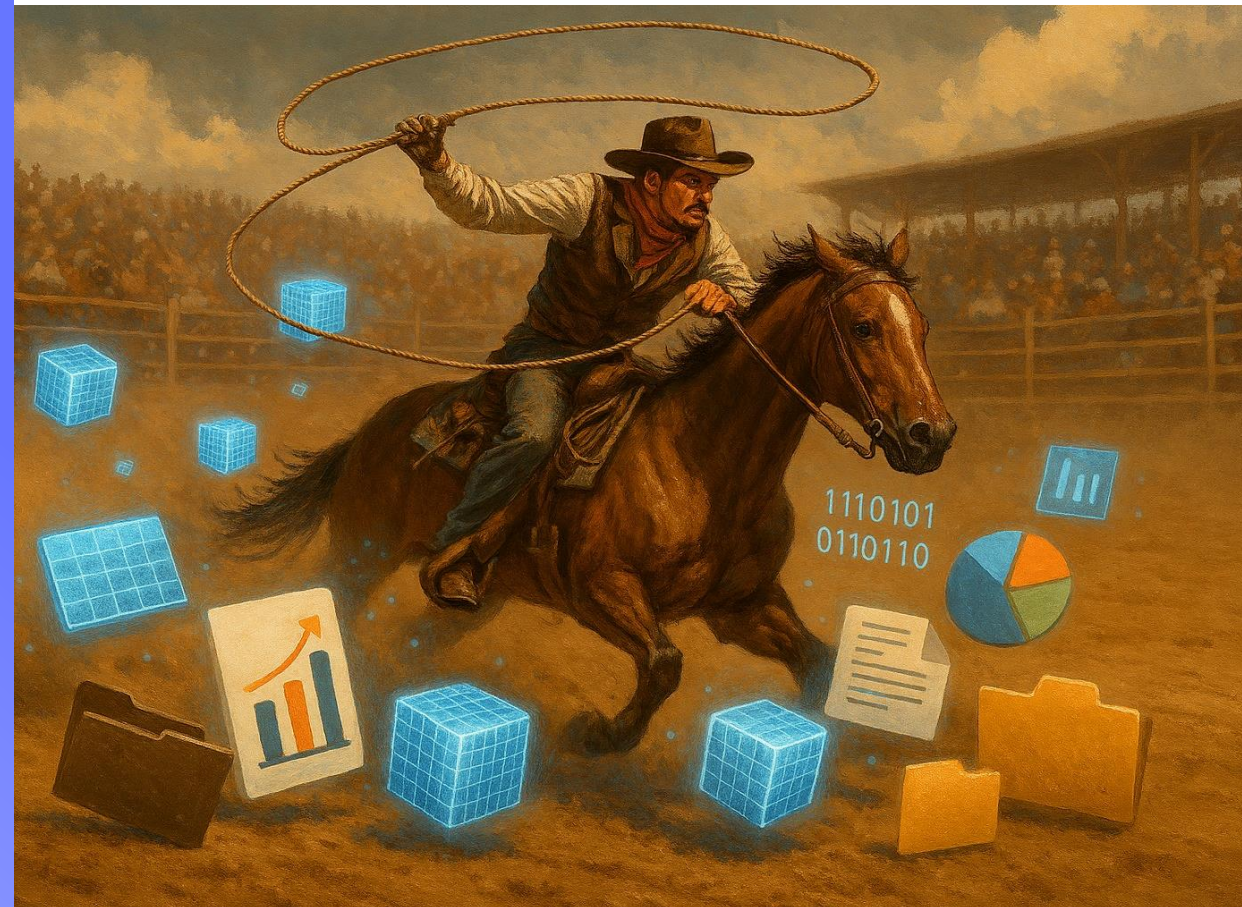


7

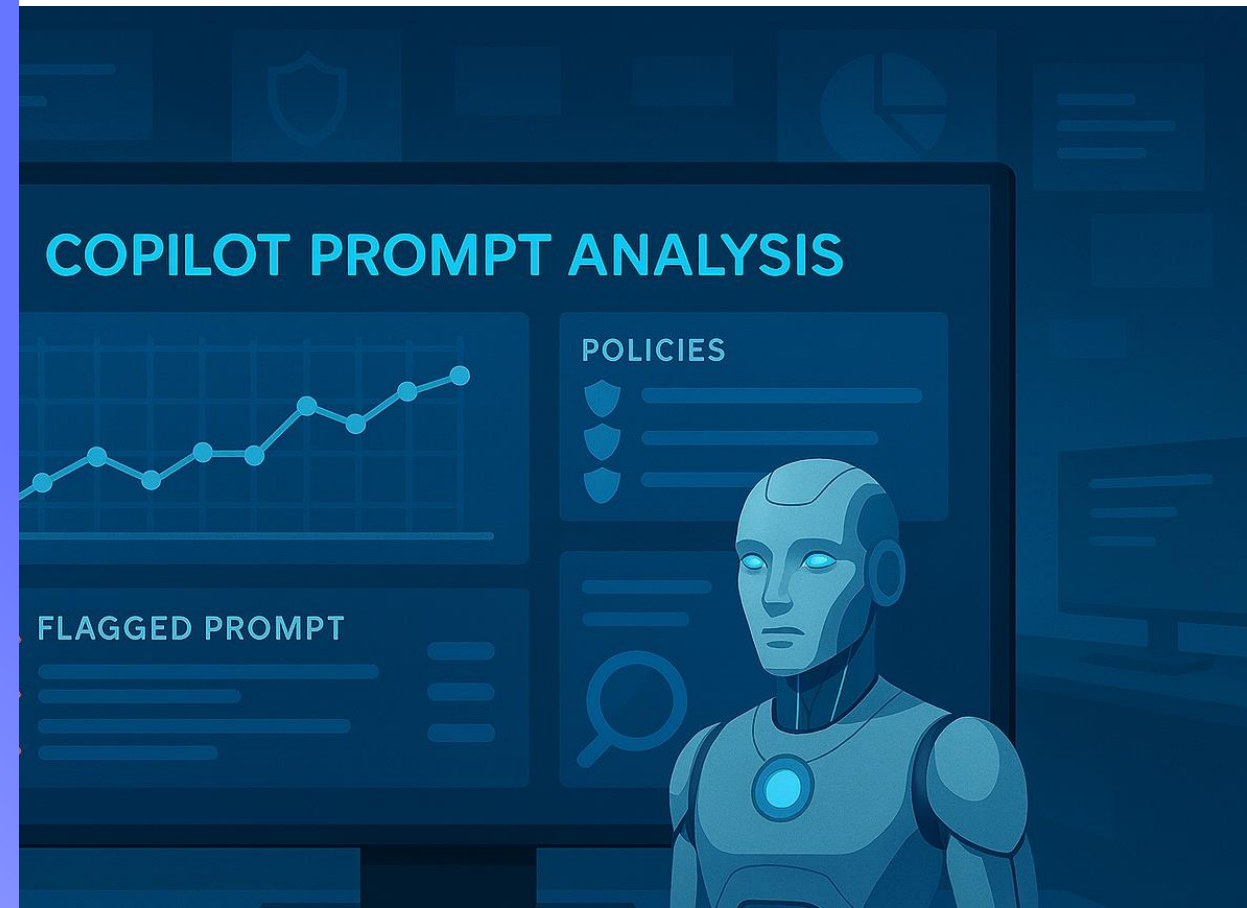
Data Lifecycle
Optimization



Data Lifecycle
Management and
Records Management



How do I
monitor how
users interact
with AI apps?



How do I govern
my third-party
AI apps and
custom
copilots?

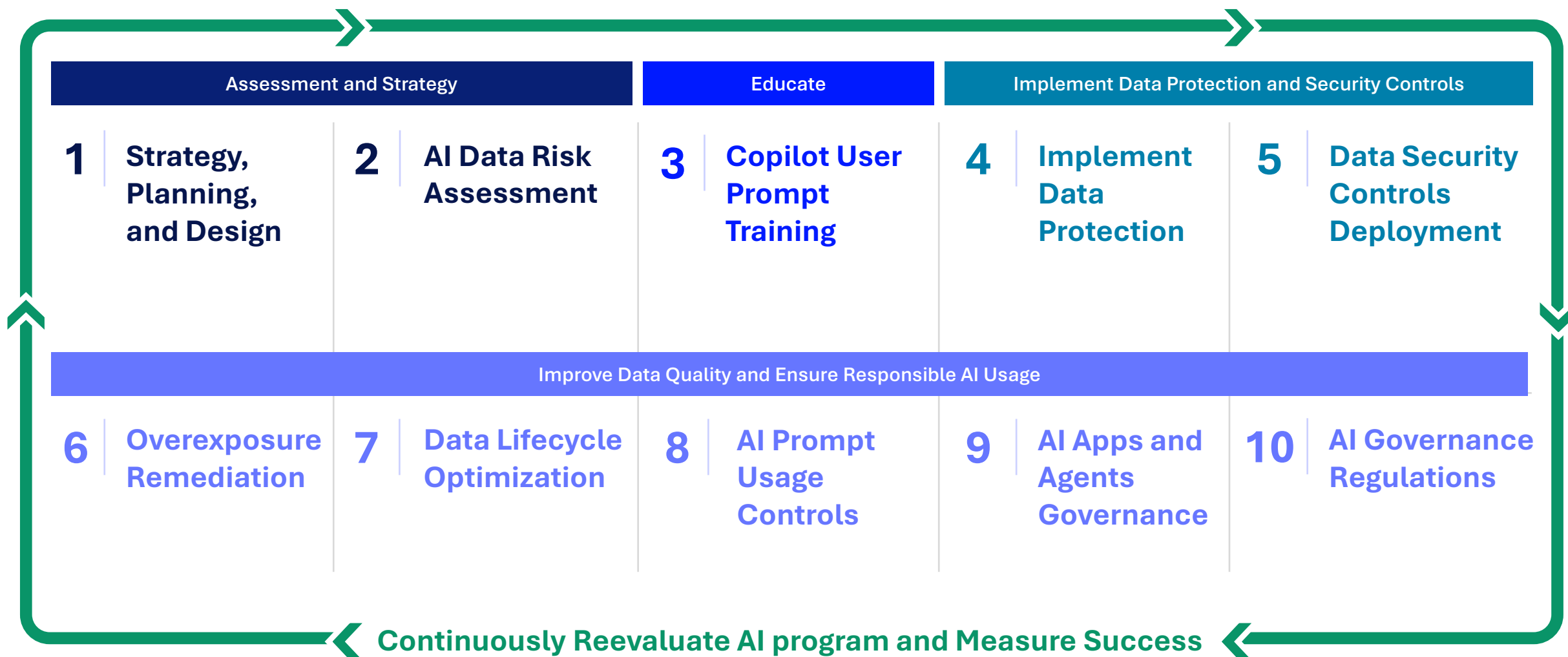


How do I
ensure my AI
tools and
usage remain
compliant?



Responsible AI and Copilot Readiness

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





epiq

Thank you.