AI security basics

Protecting your models prompts and outputs
Montserrat SemiBold

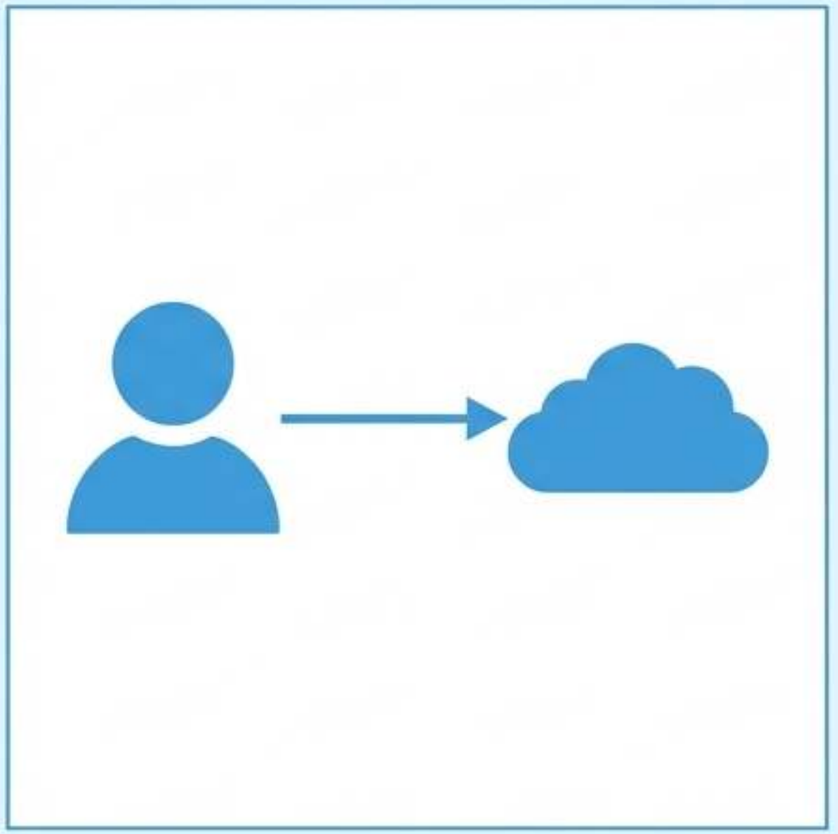
ASCENDAI®

NotebookLM

Most AI security incidents are internal gaps not external attacks



Sophisticated Cyberattack

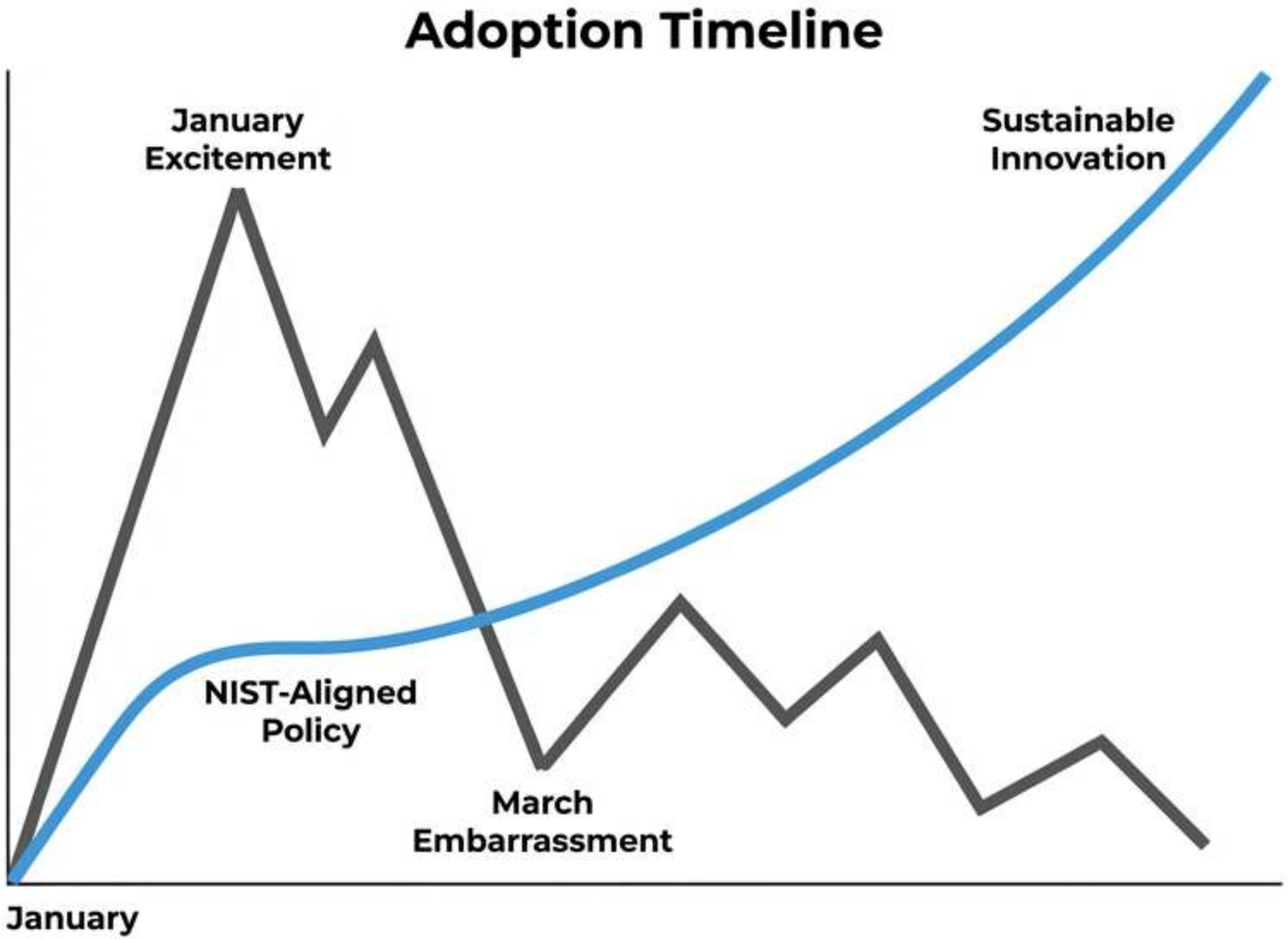


The Accidental Leak

- Employees paste client financial forecasts into unapproved chats
- Interns expose customer lists during routine system demos
- Free browser extensions log sensitive human resources data
- Nobody claims ownership over basic AI usage policies

ASCENDAI
NotebookLM

Secure foundations free your team to innovate safely



- Deploy policies and processes before testing new AI tools
- Treat security as a prerequisite rather than an afterthought
- Implement proportionate controls without requiring a CISO

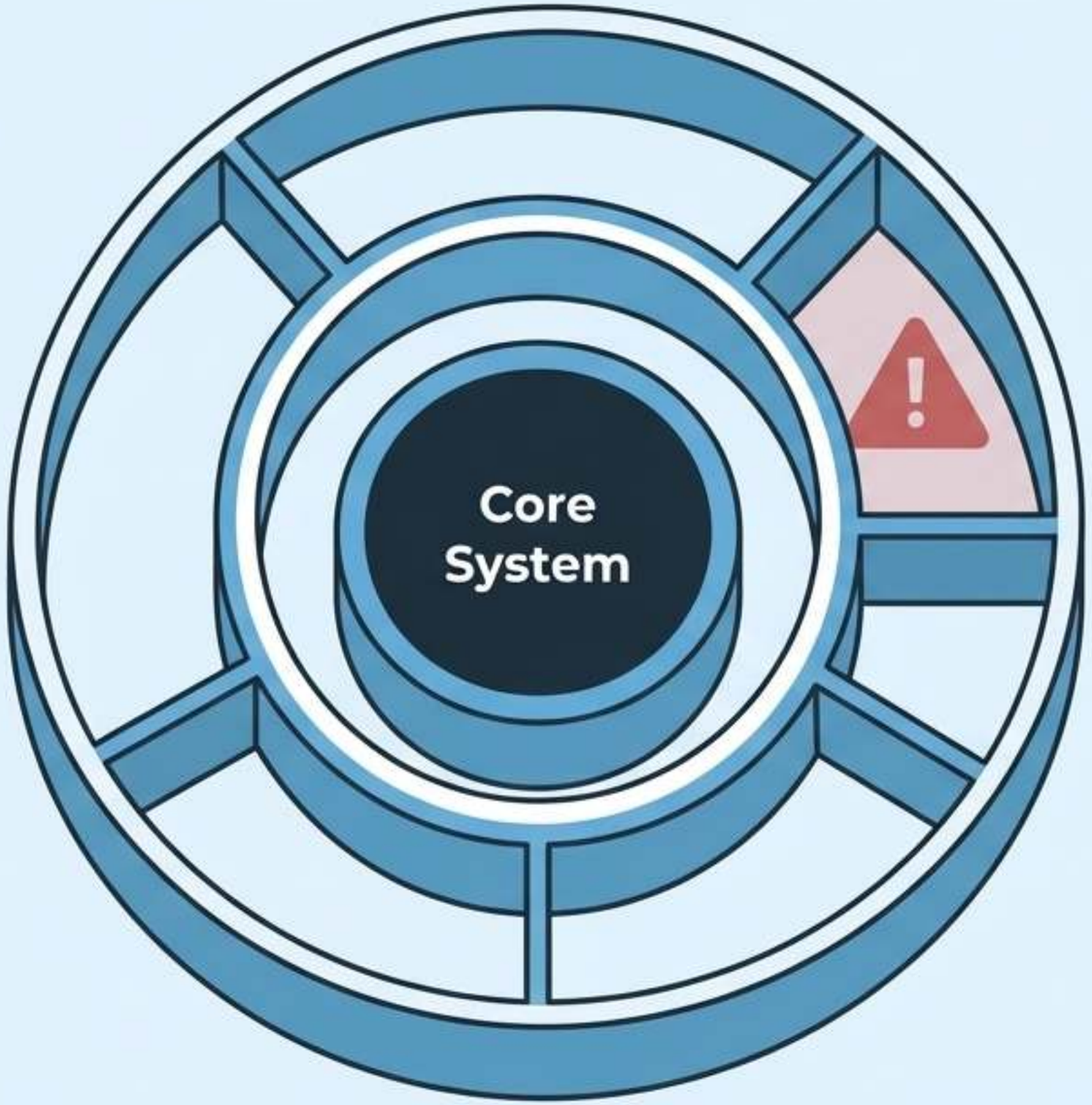
ASCENDAI
NotebookLM

Build your AI security capability in five practical steps



ASCENDAI
NotebookLM

Limit your blast radius with strict access controls



- Restrict who can use specific systems and access specific data
- Maintain a sanctioned tools register for approved experimentation
- Use role-based access to isolate incidents automatically
- Close the largest security gap without requiring dedicated cyber teams

ASCENDAI®
NotebookLM

Use placeholder data to keep sensitive information out of AI

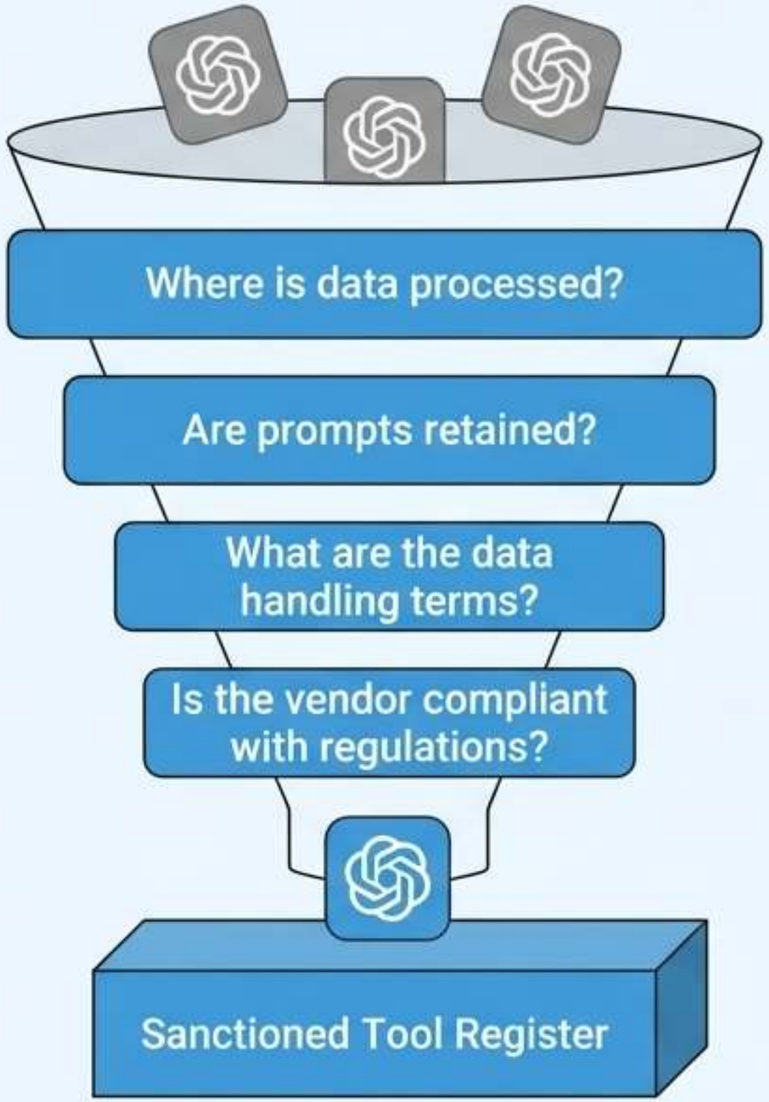


Raw Document **Sanitization Filter** **Safe AI Prompt**

- Assume all prompts are logged and used for model training
- Provide employees with safe templates featuring synthetic data
- Summarize contracts using anonymized placeholders
- Never paste identifiable client information into unapproved systems

ASCEND AI
NotebookLM

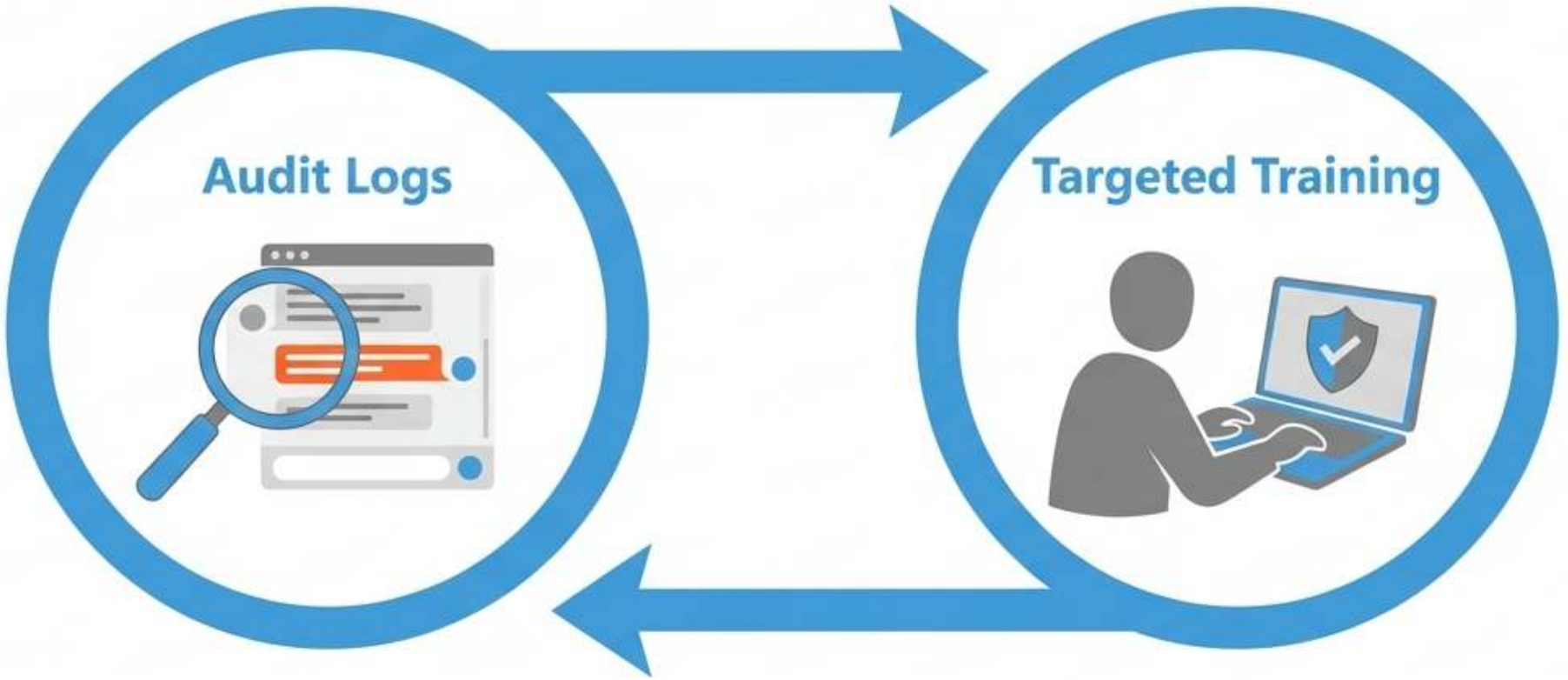
Vet every AI tool through a simple vendor checklist



- Complete basic due diligence before approving any new application
- Use a one-page questionnaire to prevent months of remediation
- Verify default prompt retention policies explicitly

ASCENDAI
NotebookLM

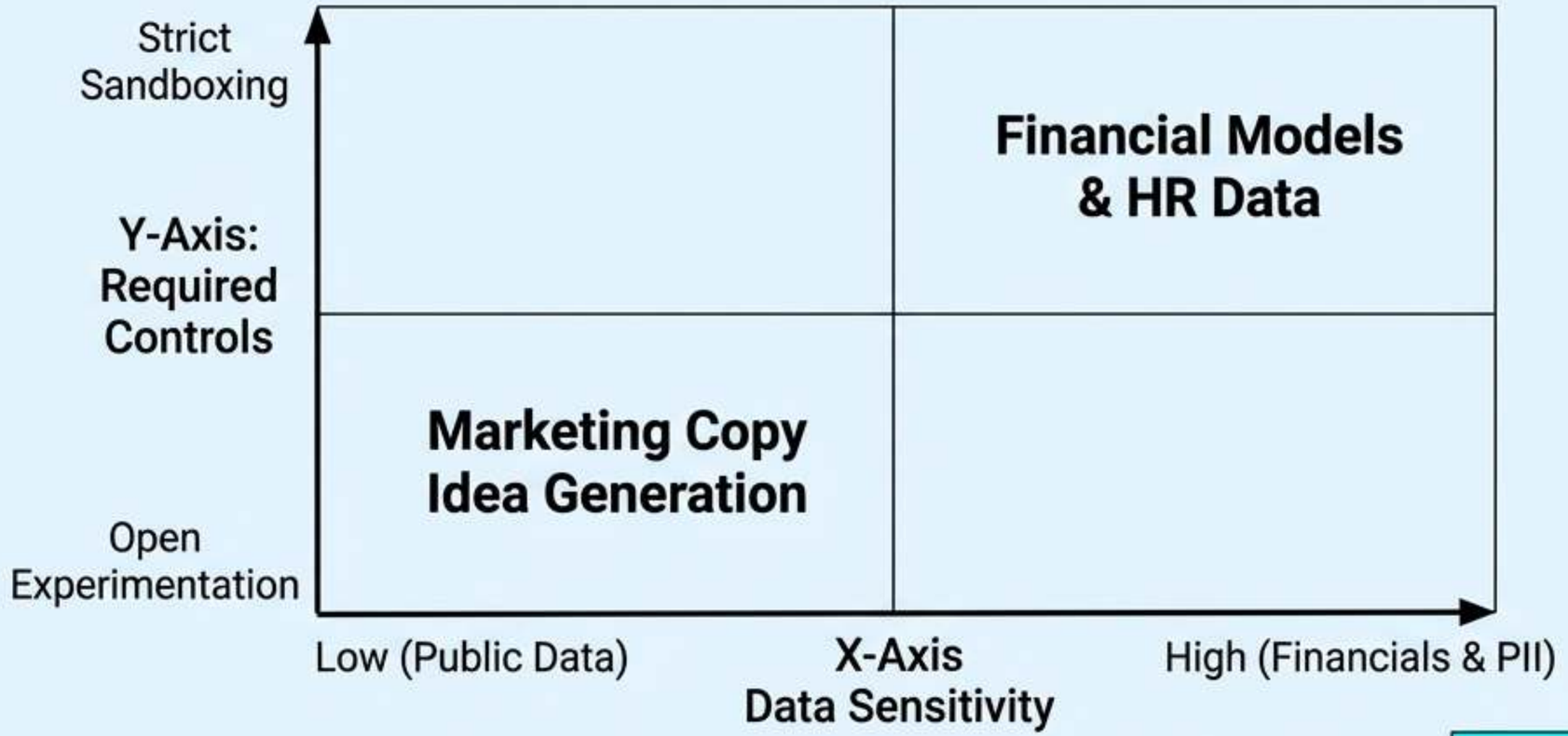
Use logging data to drive targeted hands-on training



- Audit prompts to catch inappropriate content and misuse early
- Identify repeated mistakes across teams to inform workshop topics
- Replace generic e-learning modules with actual workflow practice
- Help employees understand why controls exist so they follow them

ASCENDAI NotebookLM

Match your security controls to your data sensitivity

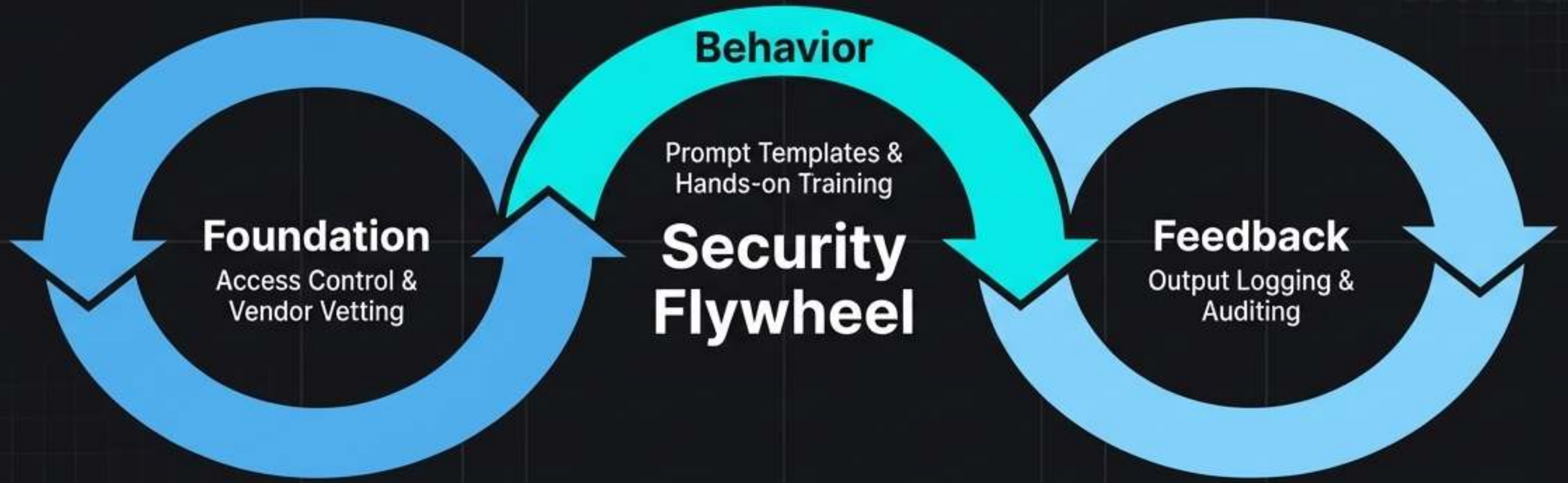


- Avoid overly tight restrictions that push teams to hidden tools
- Apply the highest scrutiny strictly where the risk is highest
- Provide teams a safe sandbox to experiment with public data

Warning: Blanket bans create Shadow AI workarounds.

ASCENDAI
NotebookLM

Transform isolated controls into a continuous security flywheel

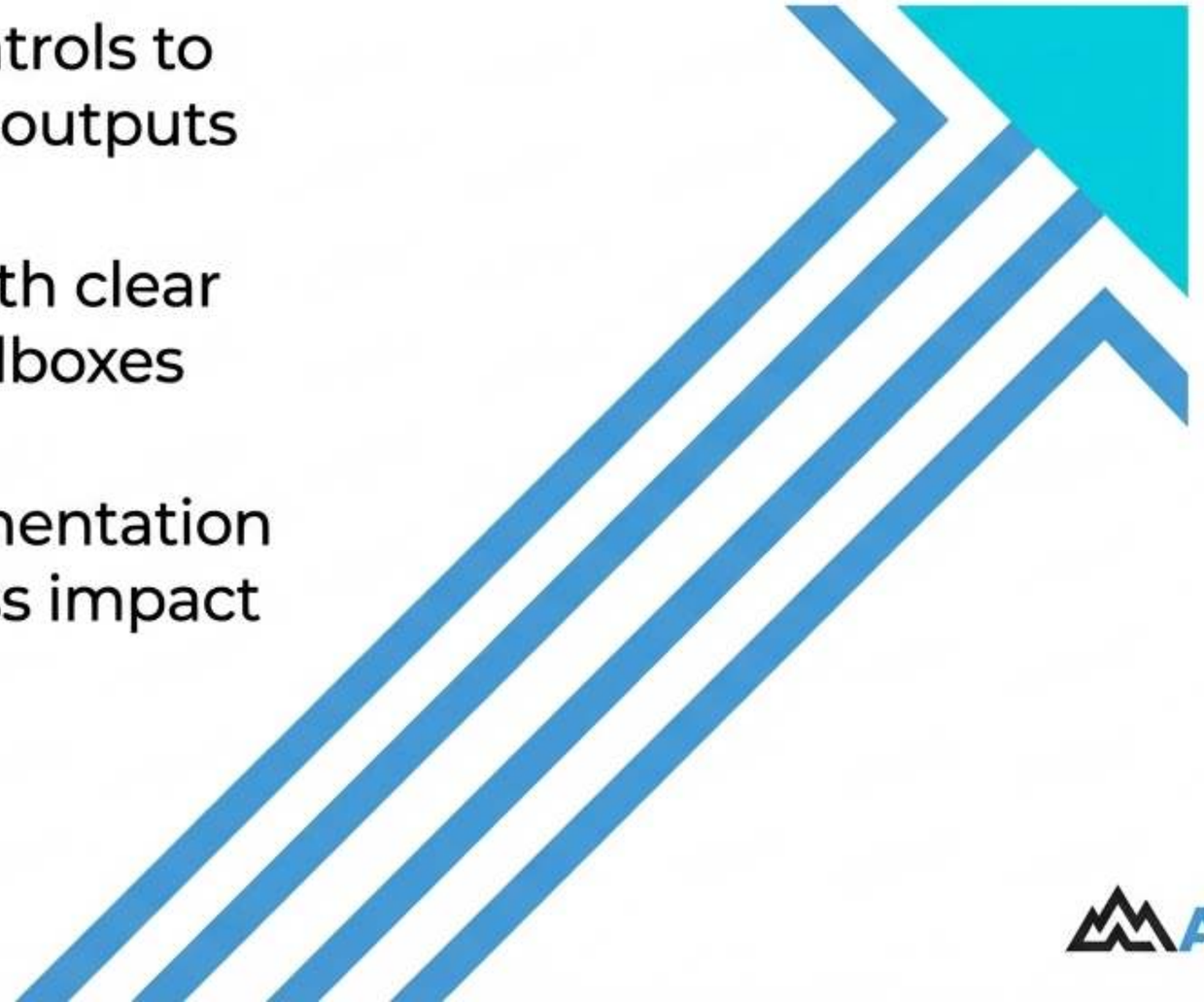


- Establish strong access and vendor foundations first
- Shape employee behavior through practical templates and training
- Use logging feedback to continuously refine your secure foundations

Ascend
secondary
NotebookLM

Build your AI capability roadmap today

- Implement practical controls to secure your models and outputs
- Empower your teams with clear guidelines and safe sandboxes
- Translate safe AI experimentation into measurable business impact



ASCENDAI®
NotebookLM