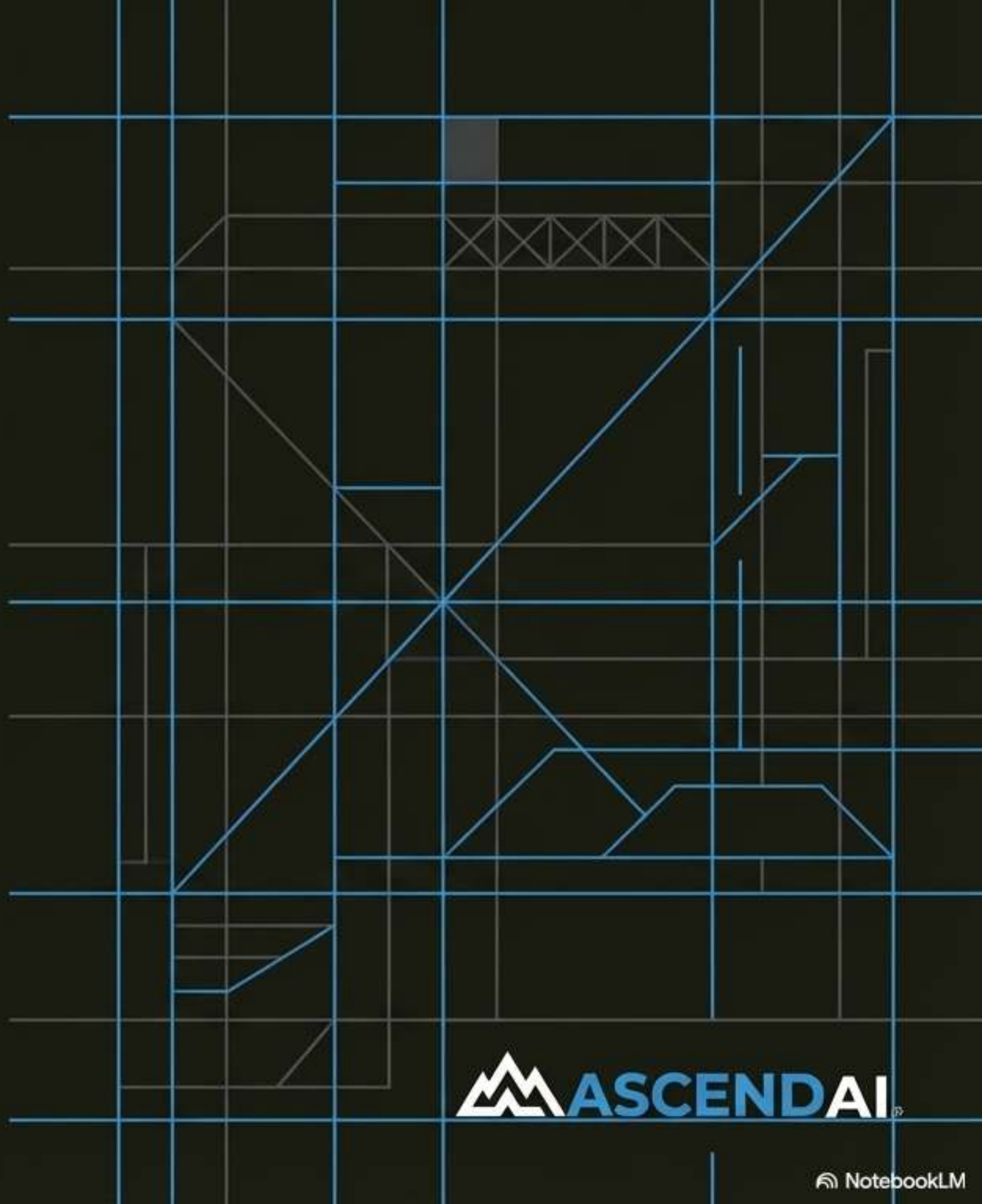
Standardize AI tools without blocking enterprise innovation

A strategic playbook to eliminate shadow AI and build an enabling governance structure

- Diagnose current enterprise sprawl
- Transition governance from gatekeeper to enabler
- Deploy the five step standardization framework

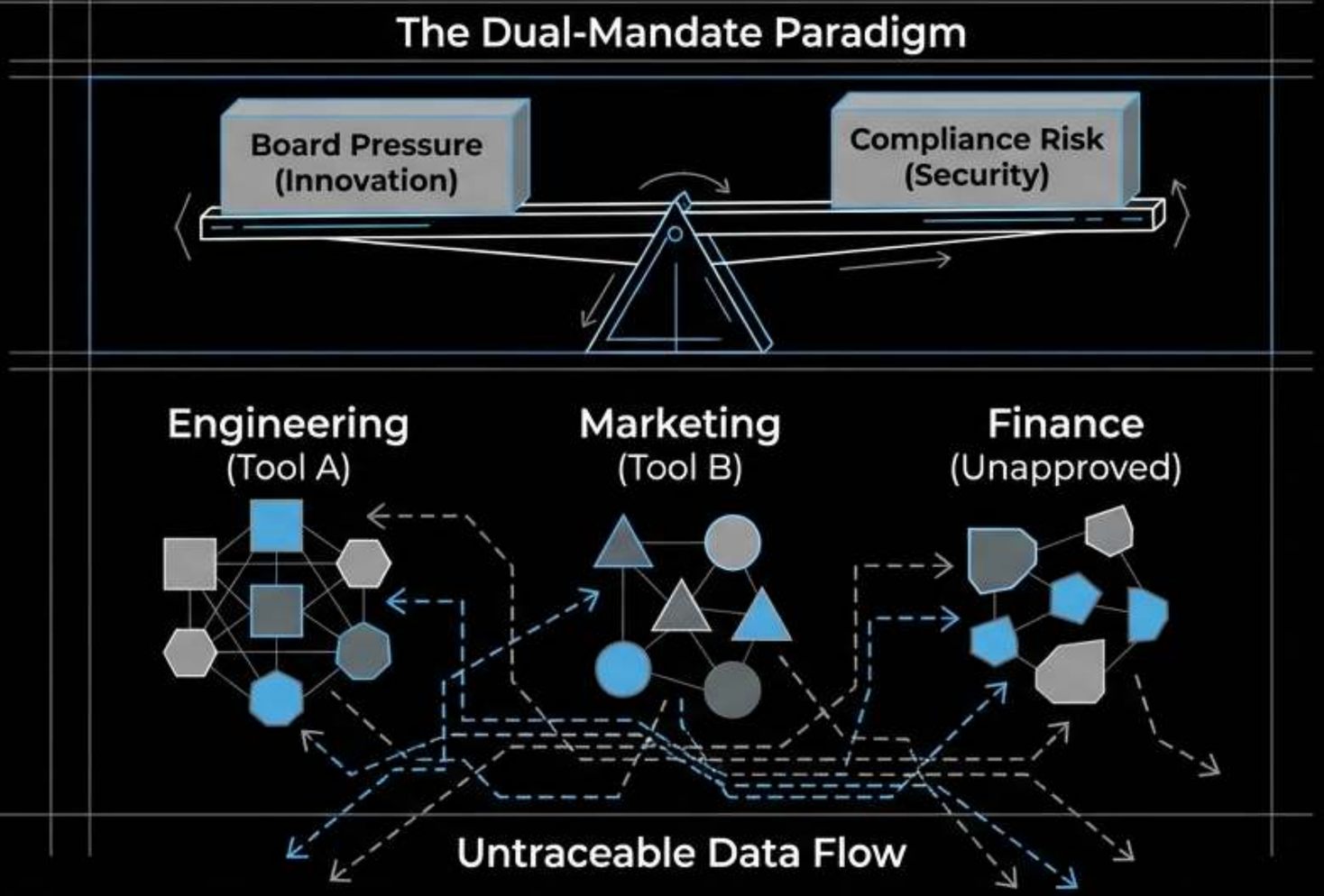


NotebookLM

The Friday afternoon reality of AI tool sprawl

Competing enterprise pressures create unmanaged, invisible risk

- Uncoordinated adoption causes fragmented data practices
- Overlapping vendor relationships increase duplicate spend
- Security gaps accumulate invisibly outside IT purview

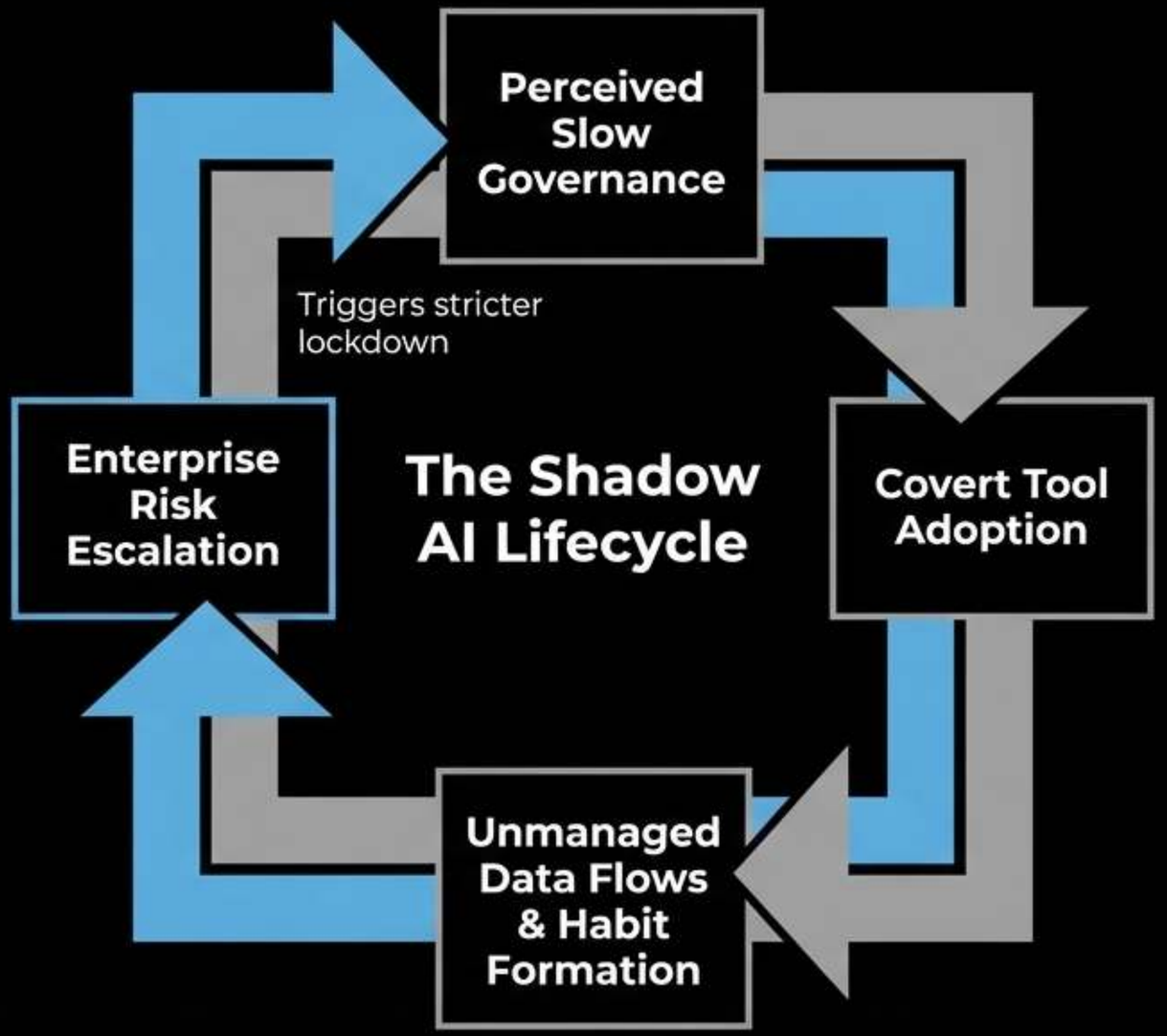


NotebookLM

Shadow AI begins when governance operates as a gate

Employees route around approval processes that ignore their immediate functional needs

- Approval processes are experienced as slow and opaque
- Employees adopt alternative tools without disclosure
- Cultural dynamics make standardization feel punitive



NotebookLM

Diagnostic comparison of AI governance models

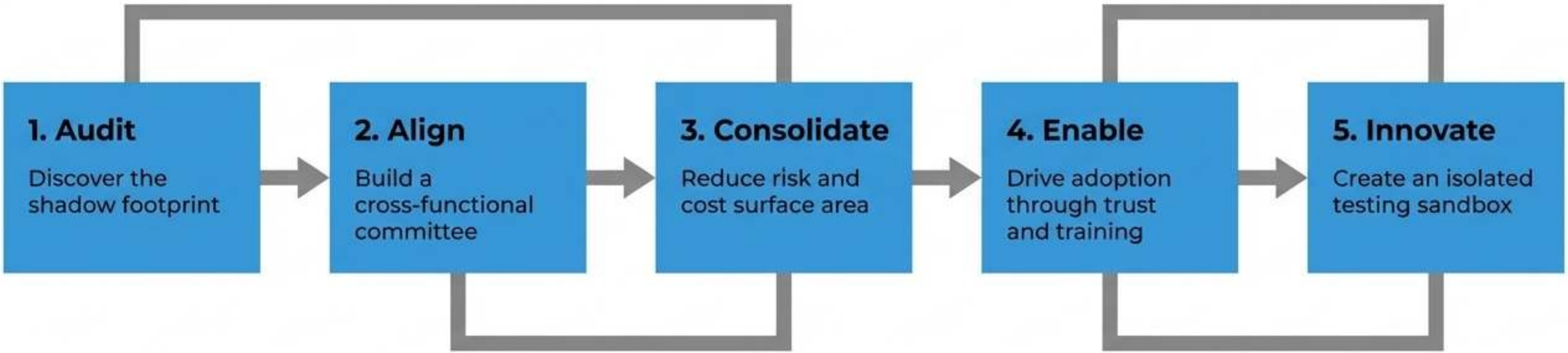
Standardisation requires shifting from punitive restrictions to strategic enablement

	The Gate (Punitive)	The Enabler (Strategic)
Perception	Slow and opaque	Fast and transparent
Integration	Disconnected from user needs	Partnered with internal champions
Action	Blocks unapproved use	Accelerates safe adoption
Outcome	Shadow AI and data leaks	Standardized stack and secure innovation

NotebookLM

The five step AI standardization framework

A sequential operating model to regain control and accelerate secure adoption



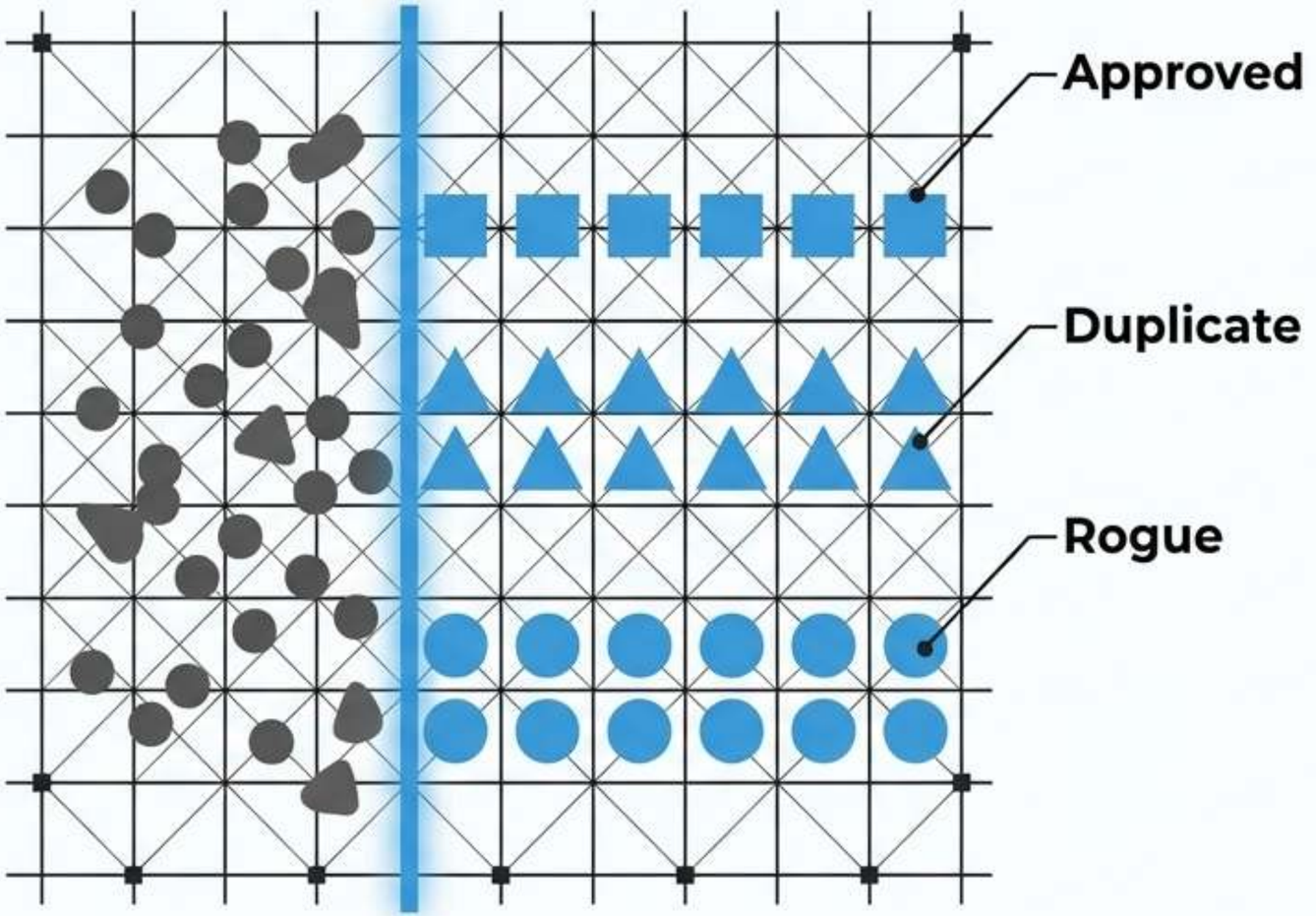
- Replaces fragmented adoption with unified strategy
- Balances global security with domain specific utility
- Transforms governance into an operational bridge

NotebookLM

Step one maps the invisible enterprise AI footprint

The comprehensive AI audit uncovers hidden risks and duplicate spend

- Document all current functions and integration points
- Map specific data flows to expose compliance gaps
- Identify overlapping tools solving identical problems
- Assess true organizational AI costs for the first time

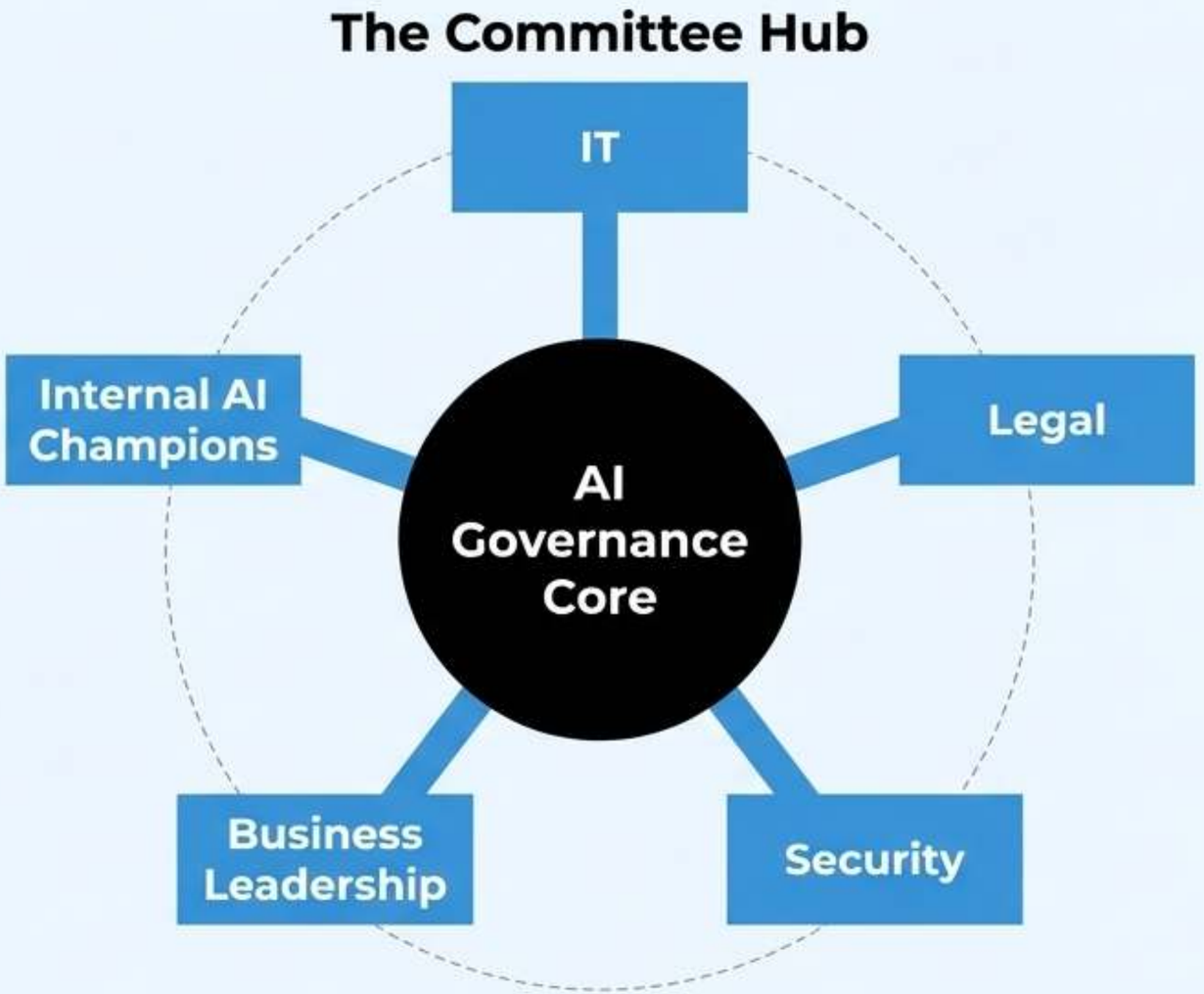


NotebookLM

Step two builds an aligned cross functional committee

Governance requires representation from risk leaders and daily users

- Position committee as an adoption accelerator
- Define clear security and compliance standards
- Evaluate tools against cost and integration compatibility
- Publish and maintain the approved enterprise stack

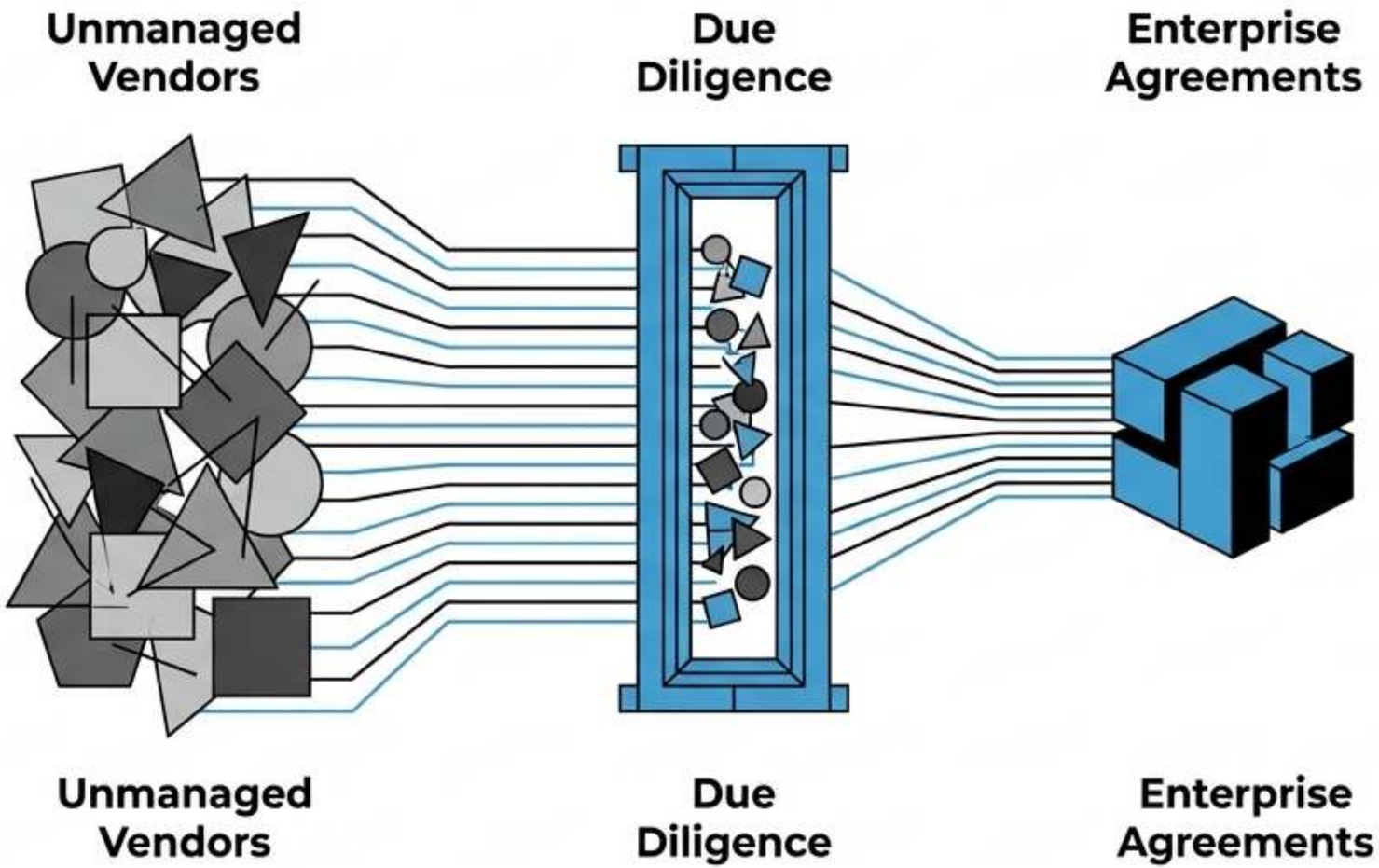


NotebookLM

Step three consolidates vendors to reduce compliance risk

Overlapping platforms multiply security vulnerabilities and integration complexity

- Reduce the total compliance and risk surface area
- Negotiate enterprise agreements where practical
- Enforce consistent data handling standards globally
- Deploy vendor due diligence for all contract renewals

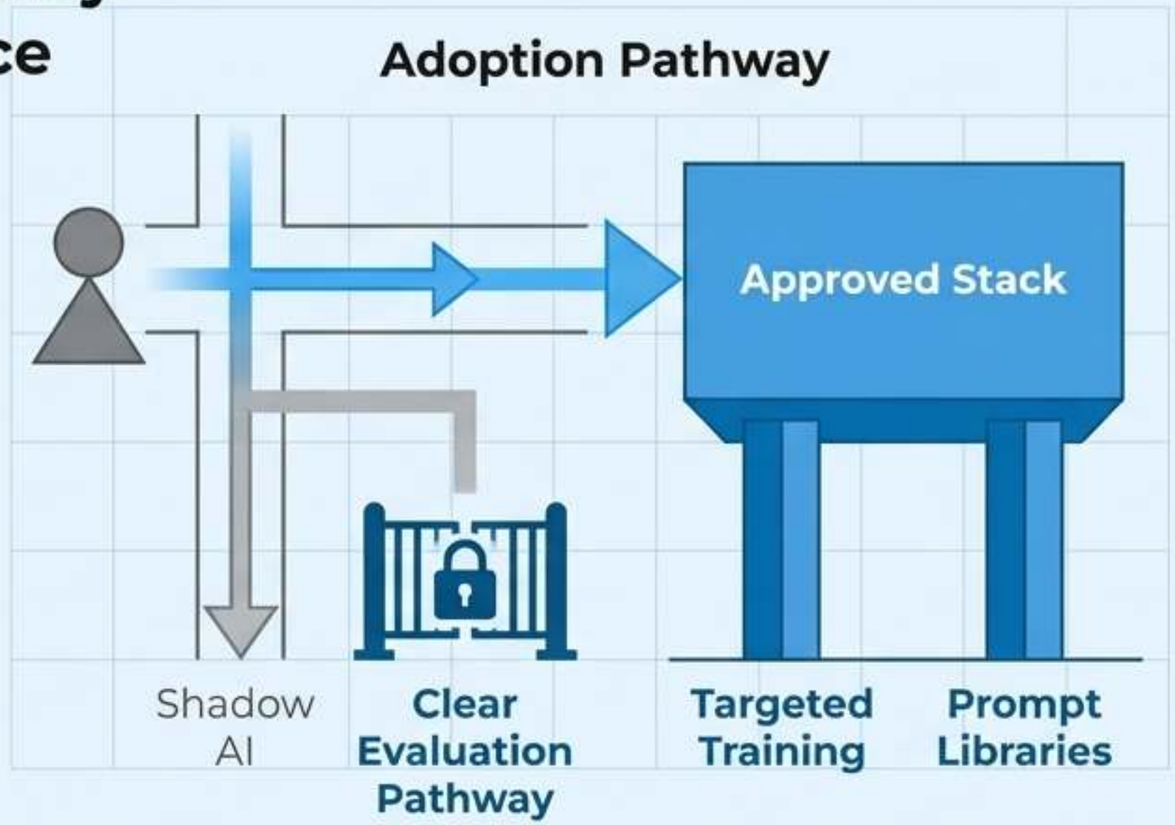


NotebookLM

Step four drives adoption through employee trust and training

Standardized stacks only survive if they are genuinely useful to the workforce

- Communicate the precise reasoning behind tool selections
- Distribute prompt libraries to maximize immediate utility
- Create transparent pathways for requesting new tools
- Collect and act on daily user feedback

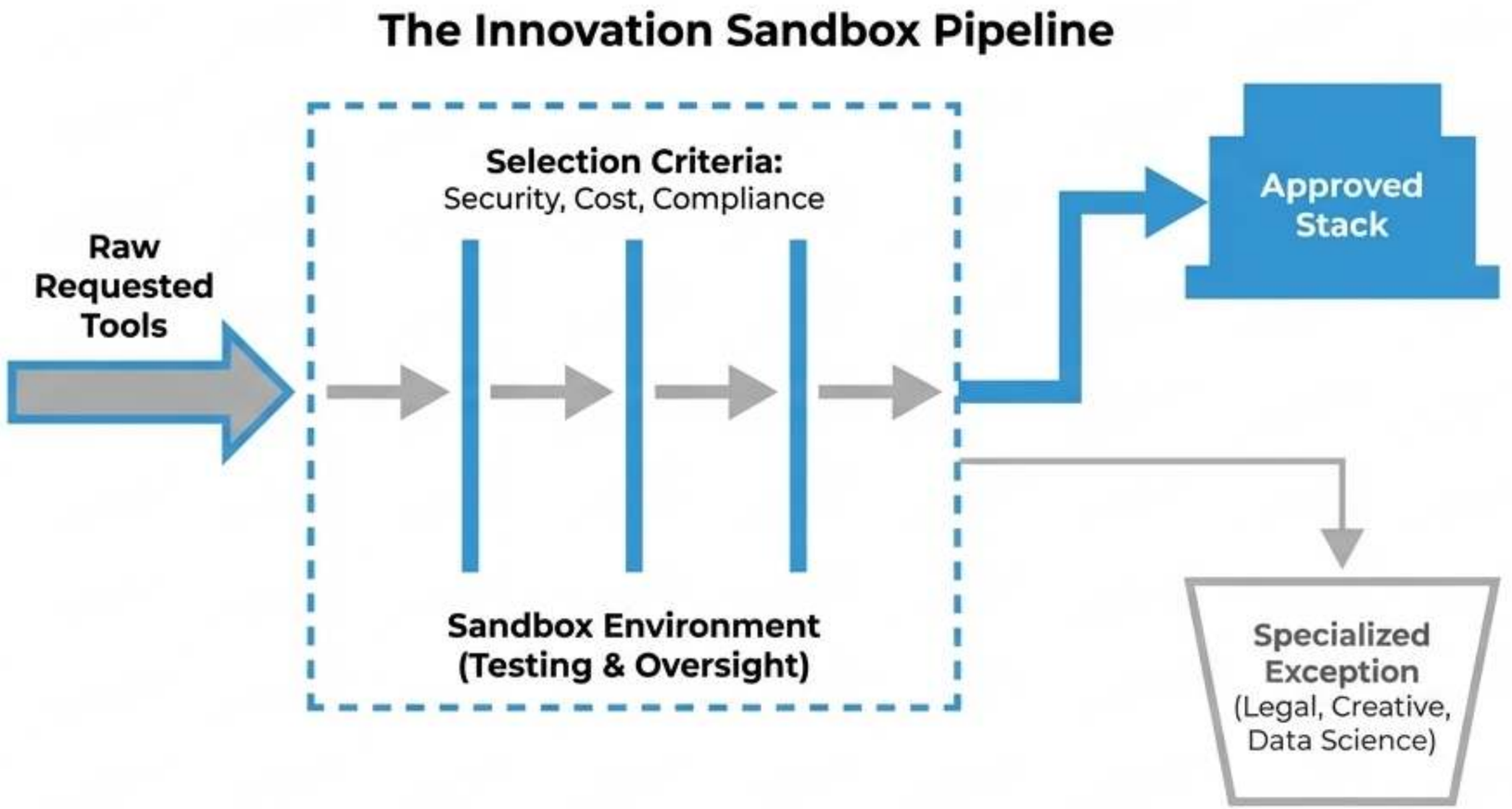


NotebookLM

Step five creates an isolated sandbox for continuous innovation

Standardisation must balance global efficiency with domain specific requirements

- Test unproven platforms under strict oversight guidelines
- Migrate successful sandbox tools to the approved stack
- Accommodate specialized functions with distinct workflows
- Treat the enterprise stack as a living ecosystem



NotebookLM

ASCENDAI

Build your AI capability roadmap

Translate AI ambition into measurable and secure business impact

- Start your enterprise AI tool audit
- Establish your cross functional governance committee
- Deploy a secure and standardized AI ecosystem

NotebookLM