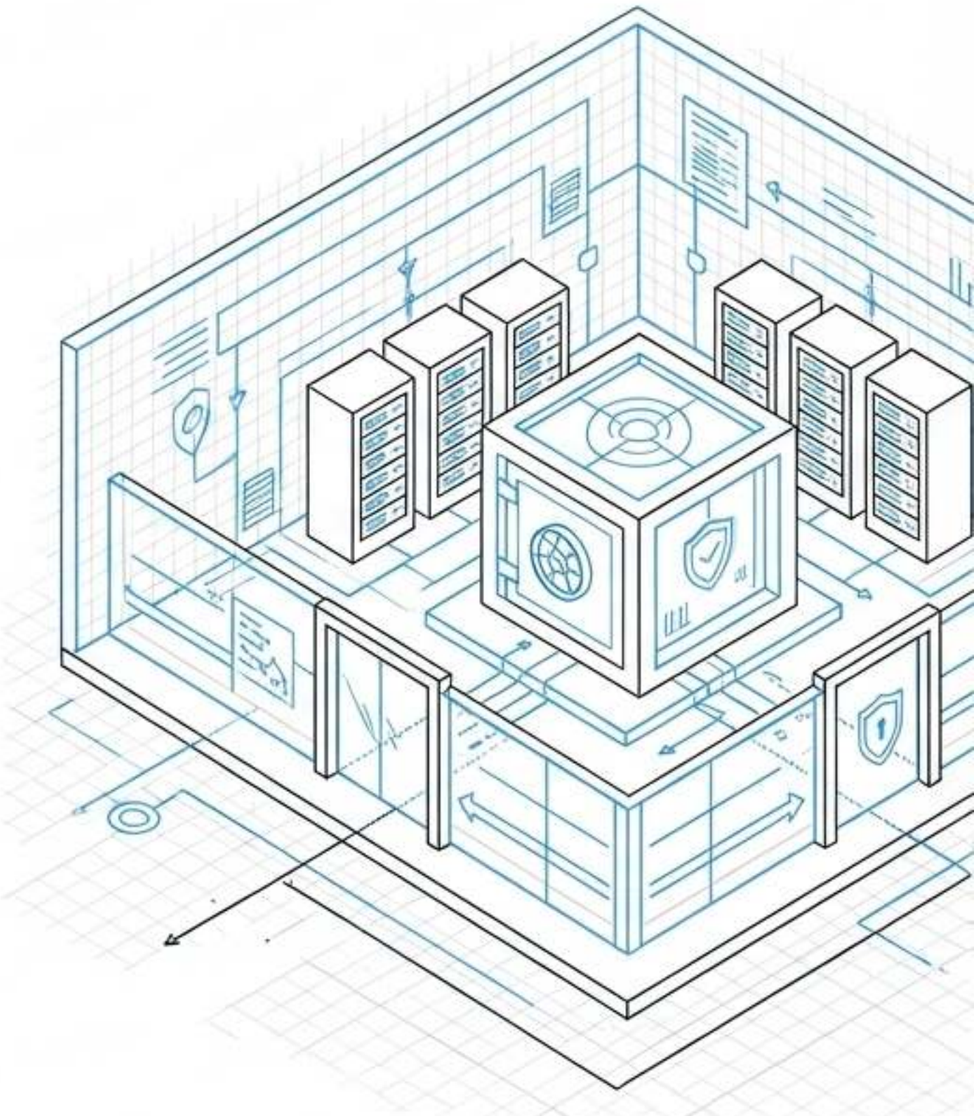
ASCENDAI

AI vendor due diligence checklist (legal + IT friendly)

A step-by-step guide to separating AI marketing hype from actual enterprise security



NotebookLM

Look beyond the sales demo

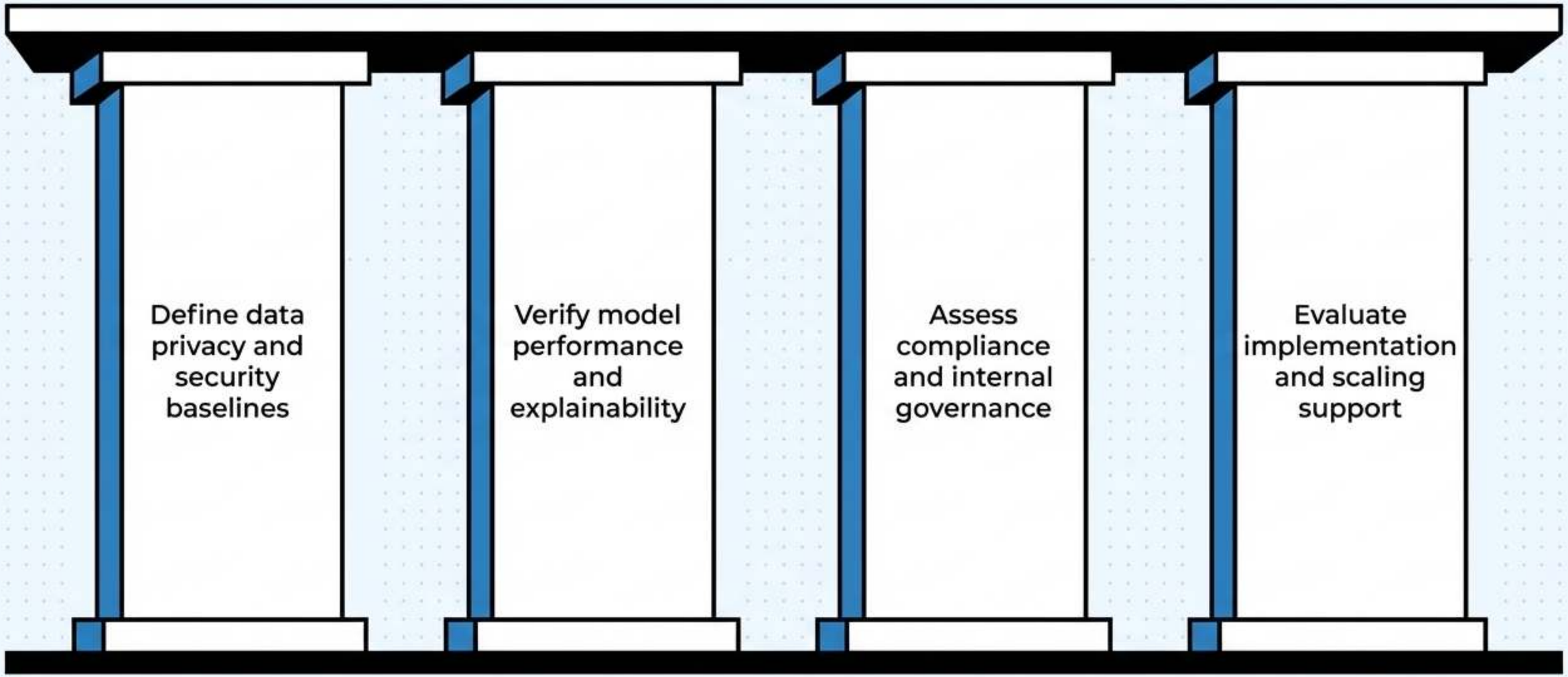
Third-party AI tools accelerate initiatives but introduce hidden enterprise risks

Marketing Promise	Enterprise Reality
✓ Highlights surface-level features	⚠ Masks critical data handling gaps
✓ Guarantees fast implementation	⚠ Obscures unvetted security architectures
✓ Promises secure and fair outputs	⚠ Hides algorithmic bias and training risks

NotebookLM

Build a repeatable evaluation process

Demand documented evidence rather than verbal promises

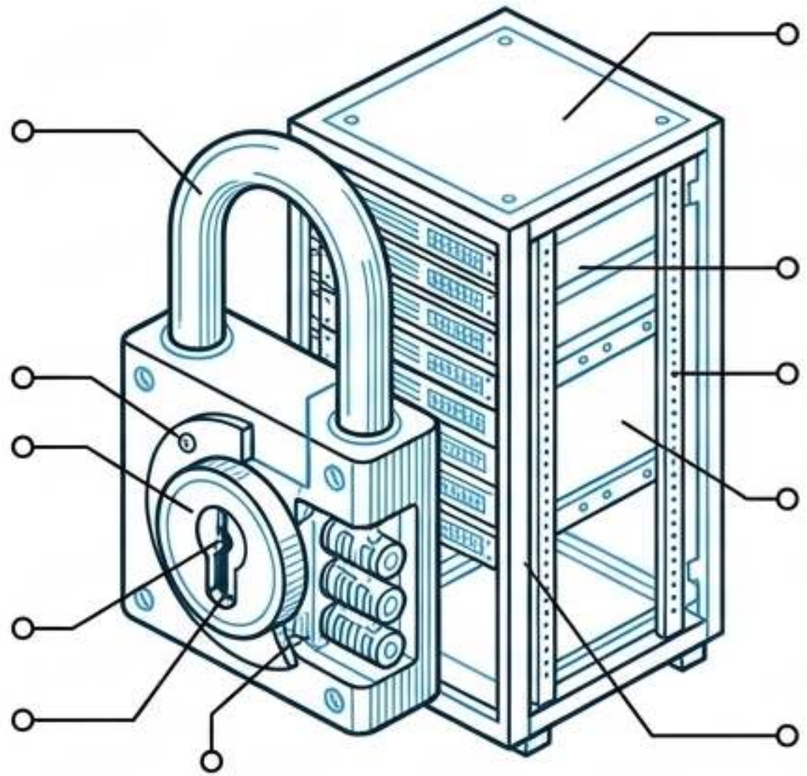


NotebookLM

Secure your data privacy and architecture

Verify encryption methods and data retention policies

- Map encryption standards for data in transit and at rest
- Define strict data retention and deletion timelines
- Confirm whether customer data trains external vendor models
- Validate adherence to recognized data protection laws



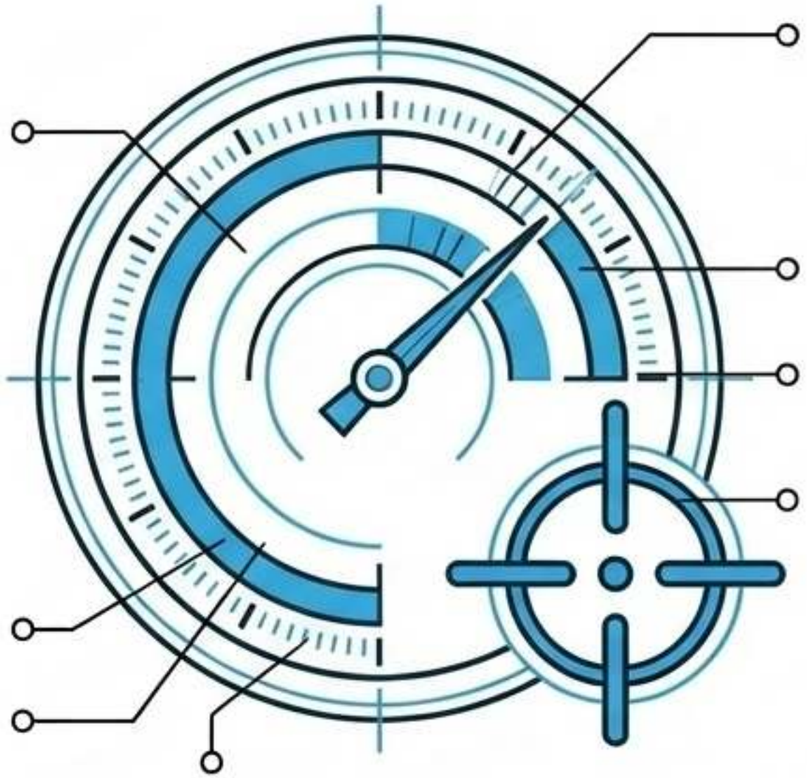
NotebookLM

02

Validate model performance and explainability

Look for alignment with NIST or ISO 42001 frameworks

- Request rigorous documentation for model training and testing
- Verify alignment with established AI risk frameworks
- Demand documented measures for algorithmic bias mitigation
- Assess vendor readiness to clearly explain model outputs



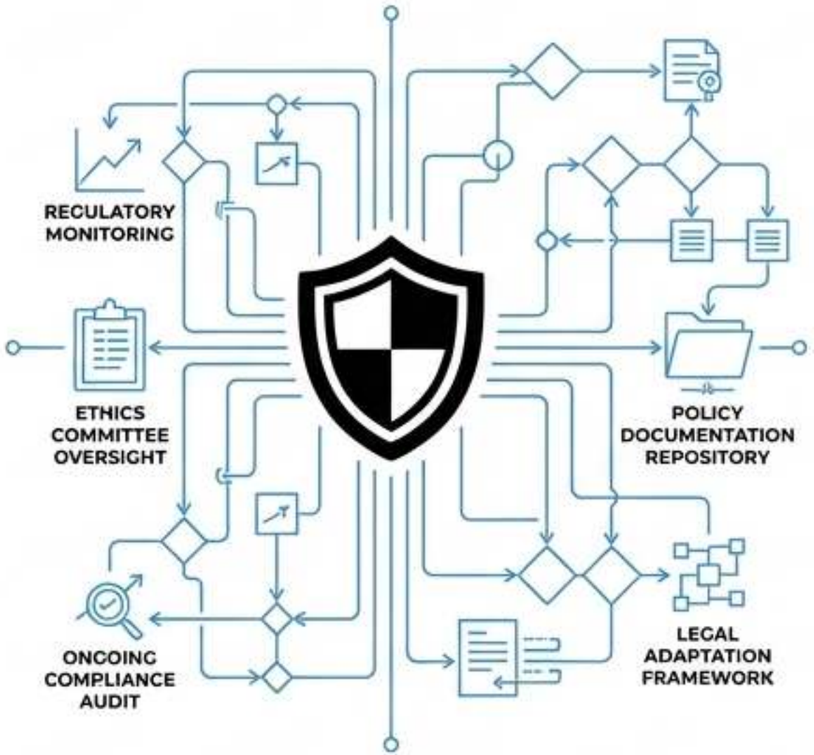
NotebookLM

03

Evaluate compliance governance and ethics

Ensure products adapt to evolving legal landscapes

- Track how vendors monitor shifting regulatory changes
- Identify dedicated responsible AI committees or ethics boards
- Require documented ethics policies over verbal assurances
- Ensure mechanisms exist for ongoing legal compliance



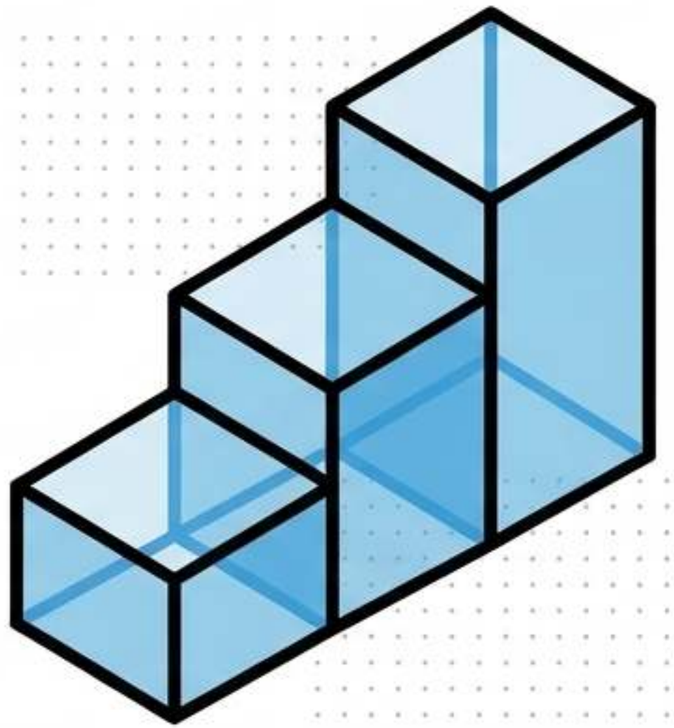
NotebookLM

04

Assess support implementation and scale

Align vendor change management with internal processes

- Evaluate vendor commitment to ongoing technical support
- Review the transparency of the future product roadmap
- Map specific technical integration and architecture requirements
- Calculate the exact internal resources required for deployment



NotebookLM

Calibrate your inquiry to the risk level

Treat the questionnaire as a living adaptable document

Risk Calibration Spectrum



Low-Risk
Productivity Tool

High-Risk
Core System

Apply a lighter evaluation touch for internal productivity tools

Use open-ended questions to reveal vendor depth and expertise

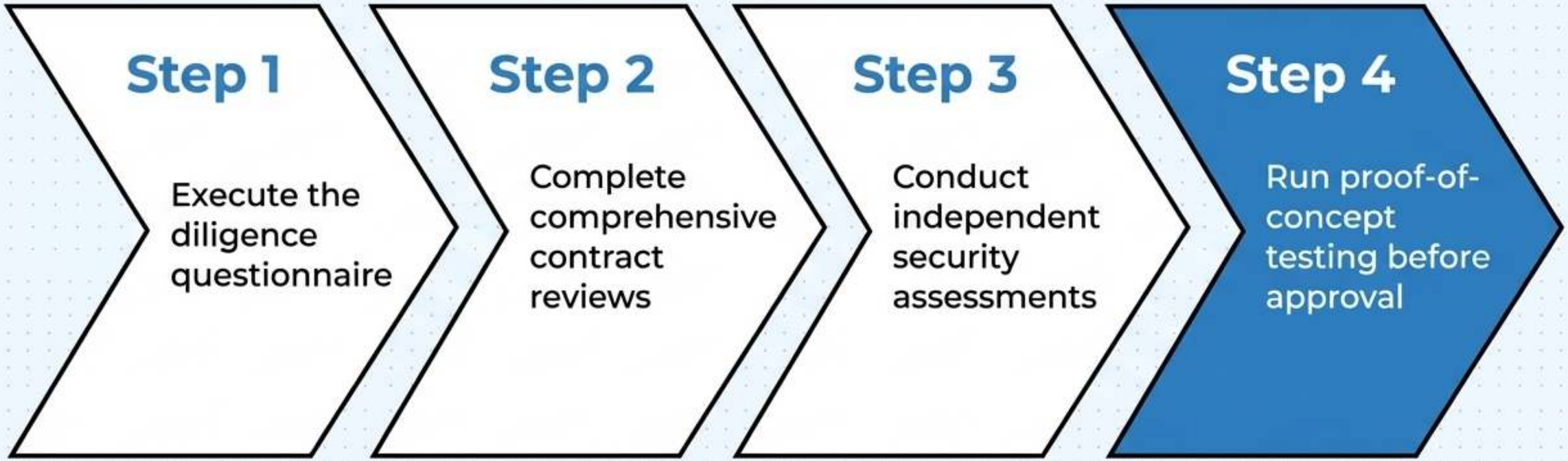
Execute exhaustive diligence for high-risk core systems

Adjust evaluation frameworks as internal risk tolerance evolves

NotebookLM

Integrate the questionnaire into the full lifecycle

A completed evaluation is only the first step



NotebookLM

Separate responsible AI from marketing hype

Demand documentation to protect your organization

- Start your AI readiness assessment today
- Build your AI capability roadmap with confidence

ASCENDAI®

NotebookLM