

5 Questions Every Security Leader Should Ask About AI Governance

As AI becomes embedded in business workflows and gains access to enterprise data, security leaders must rethink how they manage governance, accountability, and risk management. **Start with these five questions:**

1



Where does the data go, and how will it be used?

Understanding how information is stored, retained, shared, and used is essential to responsible AI adoption. Organizations should know what happens to their data throughout the AI workflow and who can access it.

What data will the system see?

Organizations should understand exactly what information an AI system can access before it is deployed. Sensitive financial, customer and business information may require additional controls, oversight or restrictions depending on the use case.

2



What systems, tools, or actions can the AI access?

As AI becomes integrated into enterprise systems, risks extend beyond information exposure. Organizations should establish clear boundaries around what the AI can access, what actions it can take and what permissions it requires to perform its role.

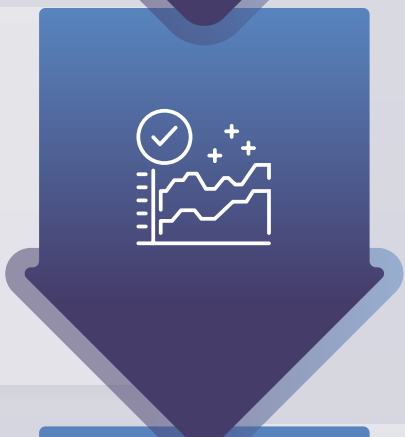
3



How are outputs tested, reviewed, and traced?

Trustworthy AI requires more than accuracy. Outputs should be explainable, reviewable and defensible. Organizations must establish processes to validate AI-generated information before it is incorporated into decision-making or regulated workflows.

4



5



Who remains accountable when the AI is wrong?

AI can accelerate analysis, drafting and research, but accountability for business outcomes remains with people. Governance frameworks should clearly define ownership, oversight and responsibility for AI-assisted decisions.

The Bottom Line

The organizations that realize the greatest value from AI will be those that balance innovation with appropriate oversight, allowing them to move faster without sacrificing trust. **DFIN Active Intelligence™ helps deal teams analyze information, surface insights and accelerate due diligence workflows while maintaining the security critical to regulatory-focused work.**

[Explore Active Intelligence](#)