

AI Governance Analyst

The AI Governance Analyst is the operational core of an AI governance program. Replace the **highlighted fields** with your specifics, trim what does not apply, and post.

Role summary

[Company] is hiring an AI Governance Analyst to operationalize responsible AI across the organization. Reporting to the [Head of AI Governance / Chief Risk Officer / CISO], you will maintain the AI system inventory, run the intake and risk-classification process for new AI use cases, and monitor controls aligned to [NIST AI RMF / ISO/IEC 42001 / internal framework]. This role sits at the intersection of risk, compliance, legal, and engineering.

Key responsibilities

- Maintain the enterprise AI inventory, including model purpose, ownership, data sources, and risk tier for each system.
- Run the AI use-case intake process: review submissions, apply the risk-classification methodology, and route high-risk cases to the review committee.
- Perform and document AI risk assessments, including impact assessments required under regulation such as the EU AI Act and [state or sector rules relevant to your business].
- Monitor governance controls, track remediation of findings, and prepare evidence for internal audit and external assessments.
- Draft and maintain AI policies, standards, and procedure documentation, and support training for business and technical teams.
- Track the regulatory landscape and brief stakeholders on developments that affect deployed or planned AI systems.
- Produce reporting for the [AI Governance Committee / Risk Committee], including inventory health, open risks, and program metrics.

Required qualifications

- [2 to 5] years of experience in AI governance, technology risk, compliance, privacy, audit, or a related second-line function.
- Working knowledge of at least one governance framework such as NIST AI RMF, ISO/IEC 42001, or a comparable enterprise risk framework.
- Familiarity with how machine learning systems are built and deployed, sufficient to hold informed conversations with technical teams.

- Experience writing policies, assessments, or audit documentation for a professional audience.
- Strong stakeholder skills: this role coordinates across legal, engineering, security, and the business.

Preferred qualifications

- AIGP, CIPP, CRISC, CISA, or an equivalent governance, privacy, or risk certification.
- Direct experience with EU AI Act readiness, algorithmic impact assessments, or model documentation standards.
- Experience in a regulated industry such as [financial services / healthcare / insurance / public sector] .
- Familiarity with GRC platforms such as [ServiceNow IRM, Archer, OneTrust, or your stack] .

About the team

[Describe the team in two or three sentences: who the analyst works with day to day, how mature the AI governance program is, and what the first year looks like.]