

AI Governance and Implementation

Paratus helps organizations adopt AI with clear decision rights, enforceable safeguards and measurable oversight.

We turn policy into daily practice so teams can pursue valuable use cases while protecting sensitive data and keeping people accountable for consequential decisions.

Three ways to engage

01

Governance baseline

Clarify ownership and priorities.

Tool and use-case inventory, risk tiers, decision rights, vendor review criteria, policy baseline and a prioritized 90-day roadmap.

02

Policy implementation

Make policy operational.

Access and data controls, approval workflows, monitoring, incident response and role-based training, with accountable owners.

03

Controlled AI pilot

Test usefulness and safeguards before scaling.

Evaluate a defined AI use case in a controlled environment. Test data boundaries, approval workflows and human oversight against agreed criteria, then document results, limitations and a recommendation on whether and how to proceed.

Grounded in a recognized framework

Our approach is informed by the NIST AI Risk Management Framework and tailored to your organization. We work alongside your business leaders, legal counsel, IT and security teams.

Experience behind the work Drawing on 25 years of technology leadership across enterprise IT, engineering, security and operational resilience.

Responsible AI programs Established policies, procedures, approved-use boundaries and AI-use monitoring for small businesses.

Private AI environments Designed and guided a controlled LLM pilot for a consulting firm handling confidential data, without a public model endpoint.

SAP-connected AI Developed safeguards for least-privilege access, data segregation, approved actions, runtime monitoring, human approval and emergency shutdown.



Let's talk about your next step

Identify your first governance priority or a use case to test.