

Operational AI Guardrails: Executive Checklist

Use this checklist to test whether your organization has moved beyond informal AI use to defined authority, safeguards, human oversight, and accountability. **A policy alone is not a governance system.**

1. AUTHORITY ■ We know who may use AI on behalf of the organization. ■ A defined person or body approves new AI tools and higher-risk uses. ■ Staff know which uses require escalation or prior approval.	2. APPROVED USES ■ Permitted, restricted, and prohibited AI uses are clearly defined. ■ Rules address both organization-provided tools and public AI services. ■ AI use is aligned with role, mission, policy, and legal obligations.
3. DATA BOUNDARIES ■ Staff know what confidential, personal, protected, or sensitive information must never enter public AI systems. ■ Data-access permissions are appropriate to the use case. ■ Vendor data retention, training, sharing, and security terms are understood.	4. HUMAN REVIEW ■ We have identified decisions that AI may assist but may not make. ■ Consequential outputs require meaningful human review before action. ■ Reviewers have authority to reject, correct, or override AI output.
5. DOCUMENTATION ■ Material AI use can be reconstructed when it influences a consequential decision. ■ Approvals, exceptions, and higher-risk uses are documented. ■ Records practices address AI-generated or AI-assisted work.	6. AUDITABILITY ■ Leadership can determine which tools are being used, by whom, and for what purposes. ■ Higher-risk systems and uses are periodically reviewed. ■ We can detect unauthorized, inappropriate, or out-of-scope use.
7. INCIDENT RESPONSE ■ There is a clear process for reporting harmful, inaccurate, biased, insecure, or unintended AI behavior. ■ Staff know when AI use must stop pending review. ■ Leadership has a response path for affected people, regulators, partners, or the public.	8. ACCOUNTABILITY ■ Named leaders retain responsibility for AI-assisted institutional decisions. ■ Governance ownership is clear across leadership, legal/policy, IT/data, HR, procurement, and communications. ■ Consequences and corrective actions exist when rules are ignored.

EXECUTIVE TEST If leadership cannot answer these questions consistently, the organization may have AI activity - but it does not yet have operational AI governance.

Need to turn the gaps into a plan?

The Guardrail Institute's 90-minute AI Governance Readiness Session helps leadership teams identify governance gaps, clarify authority and human oversight, and establish a 90-day action roadmap.

THE GUARDRAIL INSTITUTE

michael@guardrailinst.com

guardrailinst.com

Before you deploy AI, understand it.