CONVERGENT POINT STRATEGIES
AI Governance Where It Counts

Five Questions That Reveal Your Organization's AI Governance Gaps

A practical guide for leaders of mission-driven organizations

What AI Governance Actually Is — And Why It Belongs on Your Agenda

AI governance is not a technology function. It is a leadership function.

It encompasses the policies that define how AI may be used in your organization, the oversight structures that ensure those policies are followed, the risk management practices that surface exposure before problems occur, and the values alignment that ensures your AI use reflects your commitments to the people you serve.

Most mission-driven organizations have technology support — someone who keeps systems running and handles implementation. AI governance addresses a different set of questions: Which AI tools align with our mission? What are staff permitted to do with them? What does leadership need to know? What happens when something goes wrong? As AI reshapes how organizations operate, the gap between adoption and governance is where reputational, ethical, and compliance risk quietly accumulates.

> **HOW TO USE THIS GUIDE**
> Answer each question based on your current reality — not where you hope to be. After each question you will find a brief explanation of why it matters, what a strong answer looks like, and one concrete first step.

01 Does your organization have a written AI use policy?

WHY IT MATTERS

Without one, every staff member makes individual judgment calls about AI use — often without the context to assess risk. A program manager meeting a grant deadline might paste client case summaries into a free AI writing tool, unaware the platform retains user inputs for model training. The data is now outside your control, potentially violating confidentiality agreements and funder requirements — and no one knows it happened.

> **✓ WHAT A STRONG ANSWER LOOKS LIKE**
> A written policy exists, has been reviewed by leadership, communicated to all staff, and is revisited at least annually.

→ FIRST STEP

List every AI tool your team currently uses — including free, consumer-grade tools staff may have adopted on their own. That inventory is what any policy must be built on.

02 Do your leaders understand the AI risks specific to your organization?

WHY IT MATTERS

Leaders carry fiduciary responsibility for organizational risk. AI introduces exposures most haven't been formally briefed on — data privacy, algorithmic bias, vendor dependency, reputational risk from undisclosed AI use. A leader who isn't informed can't provide meaningful oversight, and can't answer credibly when a funder asks how AI is being governed.

✓ WHAT A STRONG ANSWER LOOKS LIKE

Leadership has received a substantive briefing on AI risk in the past year, understands how AI is being used in your organization, and has approved a framework for governing that use.

→ FIRST STEP

Put it on the agenda for your next leadership meeting. The briefing doesn't need to be technical — it needs to cover what AI is being used for, where the exposure is, and what decisions leadership needs to make.

03 Do you know what data your organization is sharing with AI tools?

WHY IT MATTERS

Many AI tools retain user inputs, share data with third parties, or store information in ways that conflict with your confidentiality obligations. This is an active compliance exposure for organizations serving vulnerable populations or operating under federal funding requirements. It extends beyond tools your staff chose — AI capabilities are increasingly embedded in platforms you already use, processing your data without a formal decision ever being made.

✓ WHAT A STRONG ANSWER LOOKS LIKE

Your organization has reviewed the data policies of every AI platform in use — including vendor-embedded AI — and has clear guidance on what may and may not be entered into AI systems.

→ FIRST STEP

Ask your team to list every AI tool in use. Then ask your key vendors whether their platforms now include AI features and what data those features access.

04 Is your AI use aligned with your values?

WHY IT MATTERS

AI tools learn from historical data. If that data contains bias — and most does — the AI replicates it at scale. For organizations whose work touches hiring, eligibility, or program delivery, this is a direct mission risk. An organization that publicly champions equity but uses AI tools that quietly produce inequitable outputs faces real credibility risk with funders, partners, and the communities it serves.

✓ WHAT A STRONG ANSWER LOOKS LIKE

AI tools have been evaluated against an explicit values framework before adoption, with a process in place for monitoring outputs for bias or unintended consequences.

→ FIRST STEP

Before adopting any new AI tool, ask: if this tool's outputs were made public, would they reflect the organization we intend to be?

05 Do you have a plan for when something goes wrong?

WHY IT MATTERS

Every organization using AI will eventually face an AI-related incident. The ones that navigate those moments without lasting damage had a plan before it occurred. Without one, even manageable problems become public crises when leadership is making decisions under pressure with no established protocol.

✓ WHAT A STRONG ANSWER LOOKS LIKE

A documented AI incident response protocol exists, with clear role assignments, escalation paths, and a communication strategy for affected stakeholders.

→ FIRST STEP

Walk through one scenario: a staff member accidentally shares confidential client information with an AI tool. Who is notified? Who decides next steps? How are affected parties informed? That exercise reveals exactly where the plan needs to be built.

Where Does Your Organization Stand?

Check your status on each dimension — and share this page with your leadership team.

Question	Yes	In Progress	Not Yet
Written AI use policy in place and communicated to all staff	☐	☐	☐
Leadership briefed on AI risks specific to your organization	☐	☐	☐
Data sharing inventoried — including vendor-embedded AI tools	☐	☐	☐
AI tools evaluated against an explicit values framework	☐	☐	☐
AI incident response protocol documented and role-assigned	☐	☐	☐

4–5 Yes
Strong foundation. The work now is formalizing and keeping pace as AI evolves.

2–3 Yes
Meaningful progress with real gaps. Sequencing the remaining work is the critical next step.

0–1 Yes
You are not behind because you don't care — you are behind because this is genuinely new territory.

Most organizations that work through these questions arrive at the same place: a clear list of things that need addressing and no obvious sense of where to start. That is not a failure of leadership — it reflects the genuine complexity of this terrain. The organizations that make the most progress build governance around their specific mission and risk context, and have access to expertise that translates complex AI risk into decisions their leadership can act on.

Ready to Close the Gap?

Convergent Point Strategies brings two decades of governance and policy leadership — and firsthand nonprofit board experience — to every engagement. We help mission-driven organizations build AI governance frameworks that are practical, values-aligned, and built to last.

Start with a complimentary advisory engagement — a focused conversation about where your organization stands and what a clear next step looks like.

Schedule a Complimentary Consultation →

