

AI Governance Plan Checklist

The Framework You Should've Had Yesterday

Built for leaders who know that “we’re using ChatGPT” isn’t a governance strategy.

◇ 1. Leadership & Accountability

- We’ve designated an AI leader (CAIO, CIGO/AI, or equivalent)
- Governance responsibilities are assigned beyond IT or innovation teams
- The board or executive team is briefed on AI risk and maturity
- Governance is treated as strategic infrastructure, not overhead

Pro Tip: If AI decisions are happening in silos, you don’t have governance - you have exposure.

◇ 2. Use Case Oversight

- AI use cases are inventoried, risk-ranked, and approved
- We’ve identified high-risk and prohibited use categories
- Shadow AI use is tracked and reviewed quarterly
- External AI tools (e.g. SaaS with embedded AI) are flagged and vetted

Pro Tip: You can’t govern what you don’t see. Visibility is the first control.

◇ 3. Policy & Ethics

- We have a formal AI Use Policy (covering internal + external tools)
- Our policy outlines acceptable use, review process, and ownership
- Ethical principles guide development and deployment decisions
- Team members are trained on policy relevance to their role

Pro Tip: If your AI policy still lives in a slide deck, it’s not protecting anything.

◇ 4. Data & Model Integrity

- We know what data is powering our AI (and where it came from)
- Personal, sensitive, or regulated data is controlled and documented
- Third-party models/tools are reviewed for bias, transparency, and security
- We're monitoring for drift, degradation, and misuse

Pro Tip: Garbage in doesn't just mean garbage out - it could mean fines, bias, or breach.

◇ 5. Security & Incident Response

- AI systems are covered by cybersecurity and breach protocols
- There is a process to report and respond to AI misuse or failure
- Employees are trained on AI-specific threat vectors (e.g. prompt injection)
- We have an incident response plan tailored to AI-related risks

Pro Tip: AI is part of your threat surface now - ignoring it won't make it disappear.

◇ 6. Training & Documentation

- Teams are trained on responsible AI use, not just tools
- We document rationale, decision points, and human oversight
- Governance artifacts (reviews, approvals, policies) are audit-ready
- We perform regular internal assessments or audits

Pro Tip: If it's not documented, it doesn't exist - especially when regulators come calling.

Next Step: Grade Yourself

For each category above, rate your maturity:

1 = Fire drill - 5 = Operationalized + auditable

Then ask:

What happens if we get audited... tomorrow?

What This Doesn't Include (But You'll Want):

- AI Use Policy Template
- Use Case Risk Classifier
- Vendor Review Framework
- Incident Response Playbook
- Stakeholder Alignment Map
- Responsible AI Scorecard
- CAIO-Ready Governance Operating Model

Governance Isn't Optional Anymore.

AI is accelerating. So is regulation.

If your governance plan is still theoretical, you're already behind.

Let's turn this checklist into a living system that protects your business and unlocks opportunity.

Schedule a Strategy Session Today.