GUIDE

Your Nine-Step Guide to GenAI Governance

Why Now Is the Moment for AI Governance

It didn't sneak into your enterprise. GenAI waltzed right in wearing a badge, joined your meetings, rewrote your docs, and is now quietly circulating sensitive data through tools most of your security stack can't see.

And let's be real: if you think your GenAI risk is under control because you blocked ChatGPT, Copilot is already summarizing your CFO's last 10 confidential threads in Outlook.

Why GenAI Governance FOMO is Real

Without a governance strategy, you're missing the controls that ensure integrity, accountability, and security while compliant competitors are surging ahead.

Our 9-point framework is what good governance looks like when GenAI is everywhere. Use it to build protections that scale as fast as the tools your teams are deploying.

There are four primary ways GenAI creates headaches:

- It surfaces data that users shouldn't' see
- It generates new unlabeled content that creates fresh risk vectors
- Users can share sensitive data with public GenAI, which may get ingested into its model
- It often undermines compliance with GDPR, HIPAA, PCI, etc.

The 9-Point GenAI Governance Framework

1. **Discover and classify.** Know what data your GenAI is touching, reshaping, or exposing. If you can't see it, you can't protect it.
2. **Enforce data governance policies.** Define what GenAI tools can access and what they can do with it. Guardrails, yes. Guesswork, no.
3. **Monitor and audit data usage.** Continuous visibility into who accessed what, how, and through which GenAI tool. Log it.
4. **Integrate with GenAI ecosystems.** Governance only works if it fits where your GenAI lives... in places like Copilot, Teams, Google Workspace, Slack, and beyond.
5. **Implement GenAI-aware DLP.** Prevent leaks into or through GenAI tools by understanding context, not just keywords.
6. **Ensure regulatory compliance.** GDPR, HIPAA, PCI... GenAI won't exempt you from any of them. Better governance makes the compliance journey easier.
7. **Establish accountability and roles.** GenAI governance isn't a solo sport. It's a cross-functional team game between IT, security, legal, and data leaders. Bonus points for having a centralized data risk dashboard.
8. **Train and educate teams.** Don't just block and warn. Educate users on how to work with GenAI securely and responsibly.
9. **Continuously improve.** GenAI evolves super fast. So should your governance policies. Treat them like software, not stone tablets.

Governance FOMO Checklist and Action Plan

Are you GenAI governance-ready?

- [x] Do you know where it is touching your sensitive data?
- [x] Can you trace its usage across your stack?
- [x] Is your DLP tuned for GenAI-specific use cases?
- [x] Are your audit trails GenAI-aware?
- [x] Does anyone actually own GenAI governance in your organization?

3 Quick Wins (In 30 Days or Less) For the Win

1. Run a discovery scan on GenAI-integrated content repositories
2. Review GenAI tool permissions and user access
3. Deploy one governance policy for sensitive data in GenAI tools

The bottom line

GenAI is not the threat here... lack of visibility and control is. Good governance doesn't slow innovation, it actually ensures GenAI doesn't blow up in your face.

Want help operationalizing this framework? Get in touch and we'll show you, with your own data, what good governance looks like.

Schedule a Demo