AI Governance: 5 Ways to Embed AI Oversight into GRC

As AI usage surges, organizations are right to be concerned about how it is being used and what it is being used for.

The power of AI – greater efficiency, reduced human error, and the ability to instantly analyze massive amounts of data – is undeniable. Left unchecked, however, that much power can cause significant damage to the organization in the form of privacy violations, bias, hallucinations, and model drift.

You can't put the genie back in the bottle, but you can institute AI governance practices to make sure AI is used responsibly, transparently, and fairly – without sacrificing technological innovation.

The good news is that you don't need to reinvent the wheel to govern AI responsibly. By embedding AI oversight into your existing GRC program, you can move fast, build trust – and reduce risk.

What Is AI Governance?

AI governance is a structured methodology for maintaining oversight of the use of AI to safeguard against risks and ensure ethical standards are maintained. It includes the policies, regulations, and other guidelines that govern the development, deployment, and use of artificial intelligence across the organization.

Set Your Guardrails

You may already have a strong foundation in enterprise risk, compliance, and audit. And that's the ideal place to start with AI governance. In fact, operational risk expert and frequent Risk@Work guest Dr. Ariane Chapelle cautions against creating a separate governance framework for artificial intelligence risk. "Integrate AI into your ERM framework. Try very hard to have the same framework for all your risks," she says.

AI RISKS

Hallucinations
AI has been known to answer questions with made up information.

Bias
AI uses historical information to build new content. The problem is that what was acceptable in years past may not match today's standards.

Data privacy and security
AI captures everything you type into the prompt and incorporates it into the model. Be cognizant of what information you are sharing with nonproprietary models like ChatGPT.

Model drift
The performance of an AI model will decline over time as conditions change.

Here are five ways to embed AI governance into your current GRC program.

1. **Expand risk and compliance programs to include AI-specific challenges.** Your enterprise risk, compliance, and audit programs can be extended to govern AI risks such as model drift, algorithmic bias, explainability gaps, and rapidly evolving regulatory demands. The goal is to evolve existing frameworks, not replace them.

2. **Embed governance across the AI lifecycle.** AI oversight should be integrated into every phase of the lifecycle, from model development and deployment to ongoing operations. This includes incorporating risk controls, validation checkpoints, and documentation standards at the outset, with mechanisms in place to monitor performance and compliance over time.

3. **Shift from periodic reviews to continuous oversight.** AI systems adapt in real time, and oversight must keep pace. Your governance practices must support ongoing evaluation through risk sprints, real-time monitoring, performance alerts, and other mechanisms. This allows teams to identify and resolve issues before they become business risks.

4. **Define accountability across all lines of defense.** AI governance works best when responsibilities are clearly defined across legal, compliance, audit, data science, and business teams. Embedding governance into existing functions fosters ownership, consistency, and alignment with enterprise risk strategies.

5. **Demonstrate that you're in control of AI.** Regulators, customers, and boards want evidence that AI is being used responsibly. Demonstrating control means more than documenting policies – it requires real-time visibility, traceability, and the ability to show that AI systems are performing as intended. Organizations that can prove they are in control of their AI will be better positioned to earn trust, reduce risk, and accelerate adoption.

According to a recent Riskonnect survey, 80% of organizations don't have a dedicated plan to address generative AI risks.

Don't Wait

Regulators are already taking action to ensure that AI is used safely. The EU AI Act, for instance, requires any company operating within the European Union to adhere to specific rules to ensure AI use is responsible, upfront, and transparent. The regulation categorizes usage according to the potential for harm and outright prohibits certain uses of AI as being unacceptably dangerous. The fines for noncompliance are steep.

Avoiding fines is certainly a compelling reason for establishing AI governance. But demonstrating compliance to regulators is just one factor. Consider the impact of making a major strategic decision based on undetected hallucinated data. What would happen to your competitive position if an employee uploaded trade secrets into ChatGPT to write a presentation faster?

Simply checking the compliance box will not protect you. Guardrails must be established around data privacy, security, and ethics to uphold the culture, expectations, and standards of the organization. Evolve your GRC program to accommodate these guardrails. And use technology tools to easily and consistently communicate expectations, apply policies, monitor actions, and track metrics.

AI governance cannot live within a single individual or department. It is a collective responsibility, where every stakeholder prioritizes accountability and ensures that AI systems are used responsibly and transparently across the organization. A robust AI governance program will help you strike the right balance between minimizing risk and encouraging innovation – while continuing to capitalize on all the benefits AI brings.

Important Global AI Regulations

EU Artificial Intelligence Act

EU Artificial Intelligence Act
regulates AI systems based on potential risks and the impact on society.

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

NIST Trustworthy and Responsible AI NIST AI 600-1
is a voluntary guideline to help organizations identify, assess, and mitigate risk associated with AI systems.

ISO

ISO 42001 AI Management Systems
helps organizations responsibly use, develop, monitor, or provide products or services that use AI.

For more, check out Riskonnect's AI Governance software solution.

07.25

ABOUT RISKONNECT

Riskonnect is the leading integrated risk management software solution provider. Our technology empowers organizations with the ability to anticipate, manage, and respond in real-time to strategic and operational risks across the extended enterprise.

More than 2,700 customers across six continents use our unique risk-correlation taechnology to gain previously unattainable insights that deliver better business outcomes. Riskonnect has more than 1,500 risk management experts in the Americas, Europe, and Asia-Pacific.

Visit riskonnect.com to learn more – or schedule a meeting with our experts here.

CONNECT NOW →

RISKONNECT'S INTEGRATED RISK MANAGEMENT SOLUTIONS

INSURABLE RISK
- Risk Management Information System
- Claims Management
- Billing
- Policy Administration
- Health & Safety

ACTIVE RISK MANAGER

BUSINESS CONTINUITY & RESILIENCE
- Business Continuity Management
- Operational Resilience
- Emergency Notifications
- Crisis Management
- Threat Intelligence

HEALTHCARE RISK & PATIENT SAFETY

GOVERNANCE, RISK & COMPLIANCE
- Enterprise Risk Management
- Third-party Risk Management
- Environmental, Social & Governance
- Compliance
- Internal Audit
- Internal Controls Management
- Policy Management
- Project Risk Management
- Technology Risk Management
- AI Governance
- Business Strategy

riskonnect