Is Your FI Keeping Pace with GenAI? What You Need to Do Now

Laura Miller

Generative AI isn't waiting for financial institutions (FIs) or financial services organizations to catch up. It's already embedded in vendor platforms, reshaping operational workflows, creating unprecedented efficiency gains, and generating complex risk exposures that many organizations haven't fully mapped.

The challenge isn't whether to use GenAI — it's how to integrate it responsibly as you unlock its value. The good news: according to recent survey data, most FIs are already monitoring vendor AI usage through documentation and contract language.

But monitoring alone isn't enough. Your risk management framework must keep up with GenAI risks as they evolve.

The hidden costs of AI efficiency

GenAI is a time-saver. It speeds up document processing and contract reviews and incorporates broad datasets into risk assessments, among other benefits. For lean teams managing hundreds of vendor relationships, these gains are transformative.

But efficiency has a dark side. For example, AI-generated customer communications can contain subtle inaccuracies that undermine trust, such as loan denial notices that risk fair lending violations and chatbots that provide incorrect regulatory or insurance information. Vendors may use AI without adequate transparency, creating black-box blind spots in your third-party risk program. AI tools that simply aren't accurate enough, forcing staff to recheck outputs and creating bad decisions disguised as automation.

Think of GenAI like autopilot. It can handle routine operations efficiently, but it requires constant monitoring, clear protocols for when to intervene, and drivers who understand both the system's capabilities and its limitations. FIs that treat GenAI as "set it and forget it" technology are setting themselves up for turbulence.

What You Can Do Now: Map where GenAI is being used across your FI, both internally and through vendors. Create an AI inventory that tracks use cases, data flows, and decision points where human oversight remains essential.

Navigating a complex risk landscape

Hallucinated or biased outputs can lead to significant operational risk, but that's just the tip of the risk iceberg. The real exposure comes from interconnected vulnerabilities:

- Employees sharing proprietary data in open-source AI environments.
- Third-party vendors implementing AI without adequate notice or controls.
- Compliance gaps where black box models make decisions that your institution can't explain
- Cybersecurity threats targeting AI training data to compromise model integrity
- Data privacy violations where AI processing conflicts with GLBA requirements, state privacy laws, or data minimization principles.

What You Can Do Now: Update your vendor due diligence to include specific AI-related questions. Require vendors to notify you of any AI adoption or changes. Build contract language that clearly establishes responsibilities for AI use, data handling, and performance monitoring.

Creating a strong risk management framework

GenAI requires a dynamic risk management framework — one that treats risk management as an ongoing process rather than a periodic checkpoint.

Look at the entire risk lifecycle:

- Identification should extend beyond initial vendor onboarding to include ongoing monitoring of AI adoption across your entire vendor ecosystem.
- Analysis should account for AI-specific risks, such as model drift, data poisoning, and explainability gaps.
- Treatment decisions need clear guardrails aligned with your board-approved risk appetite.
- Monitoring can't be quarterly or annual, as AI risk requires continuous oversight.

The Fintech Open Source Foundation's AI Readiness Governance Framework provides practical guidance for institutions as they develop their approach. It's designed for both technical and risk teams, covering AI across development, procurement, and operations.

What You Can Do Now: Establish a clear, written AI-specific risk appetite that guides your FI's strategy and decision-making. Ensure your board understands both the opportunities and the exposures, and that they're actively setting the tone for responsible AI adoption.

The human element in GenAI

Even the most sophisticated GenAI tools depend on human judgment. Your team must understand when to trust AI outputs and when to question them. They need to know what constitutes responsible use and risky behavior and how to escalate matters when needed.

Compliance isn't just about policies. It's about creating a culture where every team member understands their role in managing AI risk. That means regular training, clear communication about expectations, and reinforcement of responsible AI principles throughout the organization.

What You Can Do Now: Develop role-specific AI training that addresses the risks most relevant to each team. Make sure employees understand that AI is a tool that supports their work, not a replacement for critical thinking and professional judgment.

Building for what's next

GenAI adoption in financial services is accelerating. It will continue to evolve, regulations will adapt, and new risks will emerge. What matters now is building a foundation that can flex with these changes.

The FIs that are positioned for long-term success:

- Demand explainability from their AI solutions, not just performance metrics.
- Keep humans in the loop at every critical decision point.
- Treat risk assessments as dynamic documents that evolve alongside their AI footprint.
- Apply the same rigorous standards to vendor AI as they do to internal systems.
- Design governance structures with scalability.

Strong governance, continuous monitoring, and a commitment to responsible innovation aren't just compliance checkboxes. They're the difference between your FI capturing AI's benefits or becoming a cautionary tale down the road.

About Ncontracts

Ncontracts provides integrated risk management, compliance, and third-party risk management solutions to over 5,500 organizations worldwide, including 4,500 U.S. financial institutions, mortgage companies, and fintechs. The flagship Ncontracts IRM suite combines AI-powered software with expert services, helping financial institutions streamline risk, compliance, and vendor management through an intuitive, cloud-based platform. Ncontracts' Venminder solution is trusted by enterprise financial companies and other large organizations to strategically manage third-party risk across the entire vendor lifecycle.

Visit http://www.ncontracts.com or follow the company on LinkedIn and X for more information.