Navigating AI Risks: A Guide for FIs

Artificial intelligence is reshaping financial services — driving efficiency, enhancing analytics, and enabling new business models. But with these benefits come new risks. From data security and model bias to third-party dependencies and evolving regulations, AI requires disciplined oversight and strong governance.

Use this guide to assess your institution's AI risk profile and apply best practices to enhance controls, improve resilience, and align with regulatory requirements.

Category	Traditional AI	Generative AI (GenAI)
Core Function	Analyzes data to detect patterns, make predictions, or automate decisions	Generates new content — such as text, code, images, or audio — based on training data
Examples of Techniques	Machine Learning, Natural Language Processing (NLP), Speech Recognition	Large Language Models (LLMs), Diffusion Models, Transformers
Use in Finance	Credit scoring, fraud detection, document classification, voice biometrics	Drafting reports, summarizing regulations, contract analysis, customer communication
Data Dependency	Relies on labeled and structured data for training	Trained on vast amounts of unstructured data (text, code, documents)
Key Benefits	Improves accuracy, enhances risk analysis, supports decision-making	Increases productivity, reduces manual workload, improves customer engagement
Common Risks	Bias, model rigidity, limited adaptability	Hallucination, misinformation, compliance exposure, "AI washing"

Key AI Risks in Financial Services

- **Third-Party Risk**: Reliance on vendors for AI tools and services introduces exposure to data privacy breaches, opaque "black box" systems, and compliance failures if oversight is insufficient.
- **Data Risk**: Using sensitive consumer data in AI models — especially GenAI — heightens the risk of data leaks, misuse, and regulatory violations under laws such as the Gramm-Leach-Bliley Act.
-

- **Cybersecurity Threats**: AI-enabled attacks, including deepfakes, data poisoning, and automated phishing, can compromise systems and amplify cyber vulnerabilities.
- **Model Bias and Fairness Risk**: In lending or customer decisioning, biased models can lead to disparate outcomes and potential violations of fair lending and UDAAP requirements.
- **Compliance and Governance Risk**

As regulators refine AI expectations, institutions who don't include AI oversight within their risk frameworks face heightened exposure to penalties and reputational harm.

Mitigation Strategies and Best Practices

1. Strengthen Third-Party Risk Management (TPRM)

- **Due diligence:** Evaluate vendor AI models for data security, auditability, bias controls, and explainability.
- **Contract management:** Include AI-specific clauses covering usage, performance standards, compliance obligations, continuity, and exit strategies.
- **Ongoing oversight:** Monitor vendor performance, conduct audits, and require timely reporting on incidents or model changes.

2. Embed AI within Risk Frameworks

- **Governance alignment:** Integrate AI oversight into enterprise risk, cybersecurity, and compliance programs. Define risk appetite and escalation protocols.
- **Industry standards:** Reference frameworks such as the NIST AI Risk Management Framework and FINOS AI Readiness Governance Framework to guide evaluation and policy development.

3. Enhance Auditing and Accountability

- **AI audit programs:** Establish multi-layered internal audits covering governance, model management, and compliance controls.
- **Transparency and explainability:** Require documentation and interpretability for all models, ensuring decision paths can be reviewed and validated.

4. Strengthen Cybersecurity and Controls

- **Employee awareness:** Train staff to recognize AI-enabled threats such as deepfakes and phishing. Reinforce ethical AI use and escalation procedures.
- **System safeguards:** Implement threat monitoring, data minimization, and incident response measures to detect and mitigate AI misuse.

Integrating AI into the Risk Management Lifecycle

Stage	Focus
Identify	Maintain a comprehensive inventory of internal and third-party AI systems.
Assess	Evaluate data integrity, bias, cybersecurity, and compliance exposures.
Mitigate	Apply enhanced controls, updated policies, audit requirements, and staff training.
Monitor & Review	Conduct ongoing model testing, vendor assessments, and governance reviews.
Optimize for Growth	Deploy validated, well-governed AI to enhance fraud detection, customer engagement, and operational efficiency.

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.