CURATED EXCLUSIVELY
For Our Partner Network

NCONTRACTS

From Innovation to Accountability: Why AI Auditing is a Must in Financial Services

Lara Miller

When it comes to using artificial intelligence (AI) internally and across products and services, great power comes with great responsibility.

For financial institutions (FIs) and financial services organizations, the stakes around AI are particularly high: operational risk, compliance risk, reputational risk — and even ethical risk — are all wrapped up in how AI is designed, deployed, and governed. That's why AI auditing is not just a "nice to have," but rapidly becoming indispensable to a strong, risk-forward organization.

Why AI Auditing Matters

Auditing a system that thinks, learns, and adapts is fundamentally different from auditing traditional IT. AI isn't a static system; it evolves, adapts to new data, and often produces decisions that even its creators can't fully explain. That "black box" nature may unlock powerful efficiencies, but it can also conceal bias, create legal or regulatory risk, and erode stakeholder trust. For internal auditors and risk-governance teams in financial services, these gaps are flags signaling it's time for an AI audit.

An AI audit does more than check boxes: it ensures that AI-driven systems align with your organization's values, risk tolerance, compliance obligations, and long-term strategy. A robust audit framework becomes your roadmap — not just for risk avoidance, but for responsible innovation.

The Three Domains That Define a Strong AI Audit Framework

AI auditing frameworks should be organized across three interdependent domains: Governance, Management, and Internal Audit.

- **Governance** is where it begins. This is about tone at the top — defining a clear AI strategy, embedding ethical, legal, and regulatory guardrails, and ensuring any AI use supports the organization's broader values and objectives. Without this foundation, every other measure is on shaky ground.
- **Management** is execution. Once you have a strategy, management must build and enforce appropriate internal controls, oversee data integrity and security, and establish cross-functional oversight (for example, by bringing together compliance, IT, operations, risk, and business lines). This ensures that AI use does not diverge from approved parameters and that risk is actively monitored.

- **Internal Audit** is your final line of defense and your strategic advantage. Audit teams should bring independent, evidence-based reviews to AI use — evaluating risk, testing controls, assessing compliance, and advising on deficiencies. These activities are more than good compliance. They add value by shaping a more resilient, transparent, and ethical AI posture.

AI Challenges — And What They Mean for Financial Services

Deploying AI in a regulated, risk-conscious industry like finance services isn't plug-and-play. There are significant challenges:

- **The "Black Box" Problem:** Many AI models — particularly those using machine learning — lack ready explainability. For auditors, the key questions become: "How is this AI making decisions?" and "Can those decisions be justified or audited?" If not, you must document the associated risks and push for greater transparency or explainability.

- **Ethics and Bias:** AI may replicate or even magnify historical biases in data. In sectors like lending, credit underwriting, or insurance, that threat can lead to regulatory, reputational, and compliance consequences. Auditors must ensure that bias testing (both pre- and post-deployment) is part of the standard operating process.

- **Data Integrity & Security:** AI depends on data — but only if that data is accurate, properly governed, and secure. FIs dealing with sensitive personal and financial data must ensure robust data governance, access controls, encryption, privacy safeguards, and audit trails.

In short, if data is bad or governance gaps exist, AI becomes a liability, not an asset.

How to Get Started with an AI Audit

Consider these best practices as you revisit your current AI compliance practices:

1. **Ask tough, strategic questions:** What AI systems are in use today or being considered? What business problems do they solve? What risks (operational, regulatory, ethical, compliance, etc.) result?

2. **Map your AI footprint (internal and vendor):** Build a comprehensive inventory of every AI system — in-house and vendor-provided. Document data sources, data flows, system owners, use cases, and risk profiles.

3. **Establish cross-functional collaboration:** Bring together compliance, risk, technology, operations, business lines, and internal audit early. AI oversight cannot live in a single silo.

4. **Invest in training and awareness:** AI moves fast. Your team — from C-suite to audit — must understand capabilities and limitations. Training ensures everyone speaks a common language about risk, controls, and responsibility.

5. **Start with pilot audits & continuous monitoring:** Rather than waiting for perfect conditions, begin with audits of current AI deployments to assess data quality, explainability, control environment, and compliance. Then build out ongoing monitoring and review protocols.

Balancing AI Risks and Rewards

AI is not a fleeting trend — it's becoming baked into operations across financial services: customer service chatbots, underwriting engines, fraud detection, risk scoring, compliance tools, and more. FIs that embrace AI responsibly — with clear governance, robust management practices, and independent audit oversight — position themselves for scalable growth, competitive differentiation, and stakeholder trust.

Organizations that treat AI as just another technology risk, could end up facing serious problems ranging from regulatory scrutiny to reputational damage.

In an era when trust, transparency, and accountability matter more than ever, AI auditing is no longer optional. It's the foundation on which ethical, resilient, and future-ready FIs will be built.

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.