AI Policy Roundtable Report

Banking Sector Roundtable II: Policy & Governance Focus

Introduction

The roundtable was convened to facilitate a high-level dialogue on AI governance frameworks, regulatory expectations, ongoing monitoring, and the critical function of data management. This second session in the series demonstrated that regardless of an institution's size or AI maturity, several key priorities consistently emerge: governance, education, vendor oversight, and practical implementation. The session established ground rules for open discussion, focusing on the intersection of formal governance frameworks and operational reality to help bankers navigate AI adoption while fostering innovation in a rapidly evolving technological landscape.

1. AI Safety & Governance

Participants examined primary risks associated with AI implementation, specifically highlighting data privacy, security vulnerabilities, third-party vendor dependencies, algorithmic bias, model hallucinations, and regulatory compliance. There is a broad consensus on the necessity of formal governance; most institutions are currently centralizing AI policies within their broader information security frameworks and integrating these guidelines into annual employee training programs.

A significant concern involves employee conduct and the risk of complacency in digital communications. Participants noted that sensitive data in emails or notes could be indexed and unintentionally exposed by AI models, or that proprietary customer information could be inadvertently uploaded to external systems. Furthermore, vendor risk management remains a primary challenge, as many service providers integrate AI without offering full transparency into their data processing methods. Emerging competitive threats, such as Agentic AI and direct integrations by foundational model providers (e.g., OpenAI offering bank account connections within ChatGPT), further complicate this landscape.

Regarding policy development, banks are at varying stages of maturity. Some have developed early frameworks for iterative adjustment, while others have integrated AI-specific language into existing acceptable use and vendor management policies. Institutions are currently debating whether AI policies should exist as standalone documents or be integrated into existing information security programs. While some favor a dedicated AI officer, others argue that because AI is ubiquitous, a decentralized approach—distributing oversight across functional areas—is more effective for long-term integration. Ultimately, larger participants emphasized

that there is no one-size-fits-all approach; policies must be tailored to an institution’s specific size, customer demographics, and geographic location.

2. Monitoring

Monitoring practices vary significantly based on institutional maturity, ranging from risk subcommittees reviewing monthly usage reports to the use of performance metrics to categorize user proficiency. A notable challenge involves managing expectations, as younger employees often anticipate broader access to AI tools than current security protocols allow. Consequently, technical controls remain a cornerstone of monitoring, including the proactive blocking of unauthorized platforms to mitigate "shadow AI"—the use of unsanctioned tools.

Institutions are increasingly utilizing mitigation strategies such as application controls and mobile device management (MDM) to enforce compliance. A successful practice involves a "pilot" approach, utilizing technical testers who undergo specialized training to monitor usage patterns and refine controls before an enterprise-wide rollout. Furthermore, the discussion highlighted a critical gap in legacy vendor contracts, which often lack AI-specific provisions. Participants emphasized the imperative to address these omissions in future contract negotiations and renewals.

Vendor risk management was identified as a primary challenge, as many service providers now integrate AI without offering full transparency into their data processing methods. Beyond these technical concerns, the group discussed practical hurdles, such as the need for clear usage protocols for tools like Microsoft Copilot and the risk of diminished productivity if employees spend excessive time troubleshooting AI outputs.

The evolution of AI adoption since 2023 has shifted from centralized ownership to a distributed model. Participants observed that AI is a multifaceted issue spanning multiple departments. Consequently, oversight and monitoring should not reside solely with model risk management but should be distributed across the functional areas where the technology intersects with banking operations.

3. Ethics

The roundtable addressed the ethical boundaries of AI, particularly regarding the prohibition of its use in high-stakes decisions, such as credit approvals, without human oversight. Participants strongly recommended that AI policies explicitly address bias and decision-making transparency. A fundamental rule discussed was the strict prohibition of inputting non-public personal information (NPI) into public AI systems to maintain customer trust and regulatory compliance. Ethical standards are best enforced through rigorous guardrails, ensuring that AI serves as a tool for efficiency rather than a replacement for professional judgment.

4. Data Management & Preparation

Financial forecasting for AI remains difficult due to the unpredictable nature of token-based pricing, which can scale exponentially. To mitigate this risk, some institutions are exploring deterministic models. The session underscored the vital importance of data readiness; participants agreed that data must be cleaned, validated, and normalized before implementation. Many banks are currently migrating to data warehouses or cloud-based core systems to provide the unified foundation necessary for advanced modeling. This transition highlights the ongoing challenge of validating AI models over time to ensure policy enforcement remains consistent as technology evolves.

5. Resources

The session concluded by identifying practical steps for implementation and recognizing how collective support from state and industry bodies can facilitate this transition. A key observation from the discussion is that while larger banks possess more resources to invest in AI, smaller banks may hold an advantage due to greater agility and the ability to pivot processes without major IT restructuring. Participants identified a clear need for appropriate legislation that considers banking-specific requirements without creating unfair restrictions compared to fintech companies, alongside a call for continued information sharing and education through peer-group roundtables.

The following resources were identified as essential for ongoing strategy development:

- **Policy Support:** Circulation of sample policies, such as those from the American Bankers Association.
- **Education:** Development of AI training programs and board-level education.
- **AI Maturity Index:** guide bankers on the AI journey based on where they are on a maturity continuum.
- **Governance Frameworks:** Access to structured governance templates, particularly those developed by examining bodies.
- **Industry Insight:** Aggregation of third-party source data, sector-specific AI case studies, and a comprehensive industry AI playbook.
- **Readiness:** Development of an "AI Readiness Checklist" (modeled on a 12-question framework concept) to help institutions self-assess preparedness.
- **Regulatory Guidance:** NIST AI Risk Management Framework (https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf)