OCC's New "Super Intelligence" Supervisory Framework: Key Takeaways and How It Compares to the FSB's AI Sound Practices

November 11, 2026

On November 4, 2026, the Office of the Comptroller of the Currency (the "OCC") released its Supervisory Framework for Bank Use of Super Intelligence (the "AI Supervisory Framework"), which provides guidance to OCC examiners on how to evaluate banks' use of AI in business activities. The AI Supervisory Framework follows the Financial Stability Board's (the "FSB") recently released Sound Practices for Responsible Adoption of Artificial Intelligence (the "FSB Guidance"), which we discussed in our recent Debevoise Data Blog post.

While the AI Supervisory Framework and FSB Guidance address many of the same risks, the documents are written for different audiences. The FSB Guidance offers a principles-based framework for financial institutions seeking to develop responsible AI governance. The AI Supervisory Framework, by contrast, is directed at OCC examiners and provides more granular examples of how existing risk management concepts may apply to AI systems.

Although OCC Bulletin 2026-54 states that the AI Supervisory Framework does not establish new supervisory expectations, enforceable standards, or prescriptive requirements; the OCC has signaled that examiners will evaluate a bank's use of AI. Importantly, the OCC has instructed examiners to tailor their examination of banks' use of AI based on the materiality of the AI *use case*.

The OCC is the first federal banking agency to release an AI-specific supervisory framework, providing banks and other financial institutions with useful insight into how a U.S. bank regulator is approaching AI governance and risk management. Together, the AI Supervisory Framework and FSB Guidance represent an emerging approach to AI governance that emphasizes proportionality, effective human oversight, and controls addressing not only AI tools but also AI use cases.

Below, we summarize the AI Supervisory Framework, provide key takeaways from the AI Supervisory Framework and FSB Guidance, and discuss practical considerations for AI governance.

OVERVIEW OF THE AI SUPERVISORY FRAMEWORK

The AI Supervisory Framework addresses what the OCC calls "super intelligence," a term the current Administration uses in place of AI. The OCC defines "super intelligence" by referring to the existing statutory definition of AI in 15 U.S.C. § 9401(3) and the AI capabilities described in Executive Order 14434. The AI Supervisory Framework underscores the importance of administering a risk-based AI governance framework. For example, according to the OCC, high-risk use cases may warrant greater restrictions on autonomy; stronger controls; more direct human oversight and independent validation; and robust resilience measures.

The AI Supervisory Framework provides 16 components that describe how AI may affect established risk management and control areas—e.g., governance, model risk management, data protection, privacy, compliance, cybersecurity, third-party risk, operational resilience, testing, and auditability. The components are organized around six pillars:

- **Purpose**: The actions the AI system or agent is permitted to execute.
- **Risk**: The consequences if the AI system or agent's output or action is not fit for purpose.
- **Control**: Controls that may prevent unauthorized, inappropriate, or unsafe actions of the AI system or agent.
- **Oversight**: Monitoring the AI system or agent and identifying who is accountable for its use.
- **Resilience**: The bank's ability to detect, contain, recover from, and remediate AI system or agent failures while continuing critical business processes.
- **Assurance**: Evidence that AI system or agent controls continue to operate effectively.

Regarding risk classification, the AI Supervisory Framework states that AI use cases may be scored against a common set of risk factors, such that a comparable risk gets a comparable control regardless of where it originates in the bank. Risk factors include:

- Decision consequence;
- Reversibility;

- Customer / financial impact;
- Autonomy level;
- Data sensitivity;
- Explainability; and
- Provenance.

The AI Supervisory Framework includes an illustrative four-tier risk classification methodology, which would classify use cases as Critical (Tier 1), High (Tier 2), Medium (Tier 3), and Low (Tier 4). The OCC's examples of Critical (Tier 1) use cases include an autonomous payment agent and AI systems used for real-time credit decisioning, fraud-hold release, and market access. Generally, Critical use cases involve direct AI system action, limited reversibility of AI agent actions, high financial or customer impact, and autonomous or partially autonomous AI system actions. Low (Tier 4) use cases include examples like routine use of internal productivity AI tools, AI code assistance tools, and AI systems used for general employee questions. The underlying characteristic of Low use cases is that they are fully human-controlled and do not involve any exposure of customer or financial data or any direct action by an AI system.

THE AI SUPERVISORY FRAMEWORK AND FSB GS: KEY TAKEAWAYS

As noted, the AI Supervisory Framework and FSB Guidance address many of the same risks, but approach them from different perspectives. The FSB Guidance is a non-binding set of AI governance and risk management principles directed to financial institutions, whereas the AI Supervisory Framework is intended for bank examiners. Despite the difference in intended audiences, read together, the AI Supervisory Framework and FSB Guidance provide financial institutions with helpful perspective on how U.S. financial regulators may evaluate AI governance and risk management practices. Key takeaways include:

AI governance and risk management can be maintained within existing frameworks. The AI Supervisory Framework clarifies that examiners should not treat AI as a separate risk category, and banks are not required to define a separate AI risk appetite. The OCC highlights that AI can introduce, amplify, or modify risk within existing areas, such as operational, compliance, and credit risk. The FSB also incorporates AI into existing governance and risk management frameworks, and emphasizes the role of boards and senior management in AI governance.

Risk classification results in proportionate controls. Both the AI Supervisory Framework and FSB Guidance highlight risk-based AI governance, and the OCC provides an illustrative tiering methodology for use case risk classification. While the FSB Guidance does not offer a risk classification methodology, the FSB encourages financial institutions to periodically assess the materiality *and* risk of an AI use case separately.

Third-party risk management is a critical component of AI governance. Recognizing the reality that financial institutions are increasingly deploying vendor-provided AI tools and systems, the OCC and FSB each highlight the importance of third-party risk management. The AI Supervisory Framework states that reliance on AI vendors has the potential to introduce model, operational, data, legal, concentration, and resilience risks that are not fully addressed by conventional service-level and information-security reviews. The FSB recommends that financial institutions appropriately manage risks from third-party AI dependencies with a focus on performance, transparency, data quality, supply chain and concentration risks, and business continuity.

Agentic AI will increasingly impact banks' cybersecurity and operational resilience. The AI Supervisory Framework and FSB Guidance recognize agentic AI as a new attack surface, exposed to unique risks such as prompt injection, data poisoning, and agent manipulation. Notably, the AI Supervisory Framework highlights external AI agents used and operated by customers as an operational resilience risk. This is particularly relevant, as personal AI agents are an emerging issue for banks. According to the OCC, risk-based controls for external AI agents include identity, authentication, monitoring, velocity limits, dispute handling, suspension, and revocation.

WHAT FINANCIAL INSTITUTIONS SHOULD CONSIDER

Although the AI Supervisory Framework and FSB Guidance do not establish new legal requirements, financial institutions evaluating their AI governance programs may draw several helpful considerations from the documents, including:

Review AI use case inventories. Consider whether existing use case inventories capture information regarding an AI system's purpose, owner, autonomy, connected systems, permitted actions, third-party dependencies, and potential consequences of failure.

Evaluate risk classification approaches. Consider whether existing risk assessment methodologies adequately account for an AI system's ability to take action, its access to

sensitive information, the reversibility of its decisions, and its potential impact on customers or critical operations.

Assess the effectiveness of human oversight of agentic AI. For autonomous or consequential AI tools, consider whether human reviewers have meaningful authority, appropriate qualifications and expertise, and practical opportunities to identify and interrupt inappropriate actions.

Expand cybersecurity and operational resilience considerations. Consider whether existing evaluation practices address evolving AI risks, such as prompt injection, AI agent hacking, and unexpected AI agent behavior.

Review third-party risk management processes to ensure appropriate controls are applied to AI vendors. Consider whether arrangements with AI vendors adequately address model changes, data use, AI agent permissions, incident notifications, liability, and business continuity.

* * *

Please do not hesitate to contact us with any questions.



Charu A. Chandrasekhar
Partner, New York
+1 212 909 6774
cchandrasekar@debevoise.com



Courtney M. Dankworth
Partner, New York
+1 212 909 6758
cmdankworth@debevoise.com



Avi Gesser
Partner, New York
+1 212 909 6577
agesser@debevoise.com



Mari Grace
Counsel, New York
+1 212 909 6848
mgrace@debevoise.com



Kendall Howell
Counsel, Washington, D.C.
+1 202 383 8013
khowell@debevoise.com

This publication is for general information purposes only. It is not intended to provide, nor is it to be used as, a substitute for legal advice. In some jurisdictions it may be considered attorney advertising.