KPMG

Regulatory Alert

Regulatory Insights for Financial Services



November 2026

Super Intelligence: OCC Supervisory Framework for Bank Use Cases

KPMG Regulatory Insights

- ***Consequence-Based Controls:*** *Ties control intensity to the potential consequences of an SI model's or agent's failure or misuse, rather than technical sophistication; risk factors include the level of autonomy, human oversight, reversibility, data sensitivity, and provenance.*
- ***Existing Frameworks:*** *Does not treat SI as a separate risk category and does not expect banks to define a separate SI risk appetite; the supervisory framework may help to identify where SI introduces, amplifies, or modifies risk in a bank's normal course of business.*
- ***Living Framework:*** *Updates to the framework are expected as technology, use cases, and supervisory understanding change and mature; examiners will apply judgment based on each bank's size, complexity, and risk profile.*

The Office of the Comptroller of the Currency (OCC) issued a supervisory framework for examiners to use when evaluating banks' use of "Super Intelligence" (SI)* in normal-course activities, such as credit decisioning, payments, fraud detection, customer service, operations, risk management, and market activities, and the banks' associated risks and controls. Notably, the OCC states that SI should not be treated as a separate and distinct risk category and banks are not expected to define a separate SI risk appetite. Rather, the OCC expects that SI's contribution to existing risk categories should be addressed within banks' risk management frameworks.

The SI framework is comprised of 16 components organized under six pillars that identify principal supervisory considerations. A risk tiering methodology and a technical lexicon are also provided to supplement the framework.

**Note: Executive Order 14434 directs departments and agencies to use "Super Intelligence" and "SI" in place of "Artificial Intelligence" and "AI" in official correspondence, public communications, websites, reports, policy documents, and other non-statutory documents within the executive branch.*

KPMG

© 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights

Supervisory Framework on Banks' Use of Super Intelligence

Pillar 1: Purpose *Defines the actions the SI system or agent is permitted to execute*

Component	SI-Specific Considerations to be Evaluated
Defined Purpose & Permitted Use	— Define and document SI risk management. — Establish the authorized scope of an SI system or agent. — Provide a basis for identifying scope drift, unauthorized use, and control failures.

Pillar 2: Risk *Assesses the consequences if the SI system or agent's output or action is not fit for purpose*

Component	SI-Specific Considerations to be Evaluated
Risk Classification & Criticality Assessment	— Analyze each SI use case through "consequence-based" assessments (e.g., reversibility, customer impact, interdependencies).

Pillar 3: Control *Identifies controls that may prevent unauthorized, inappropriate, or unsafe actions of the SI system or agent*

Component	SI-Specific Considerations to be Evaluated
Human-in-the-Loop & Human-on-the-Loop Controls**	— Define the nature and level of human oversight and human involvement calibrated to the potential consequences, autonomy, reversibility, and operating volume of the use case. — Demonstrate that the control operates as intended.
Model Risk Management Extensions	— Adapt certain model risk management principles to a use case's risk factors, including potential consequences and reliance on third parties or continuously updated models. — Consider alternate benchmarks, reference sets, expert reviews or controlled comparisons for testing outputs.
Data Governance	— Assess the quality, lineage, representativeness, and permitted use of data used to train, fine-tune, and operate an SI system. — Consider both data provided to the SI system and new data created through prompts, outputs, embeddings, logs, feedback, or synthetic generation. — Monitor for changes in input populations or data distributions that may degrade outcomes.
Privacy	— Map privacy considerations (e.g., permissible use, data minimization, consent) to each use case and revisit when the model, provider, data, or purpose changes. — Establish access controls and risk-based retention periods. — Clarify, in contracts and technical configurations, the acceptable uses of bank data.
Compliance	— Consider compliance through design, development, procurement, deployment, monitoring, change management, and retirement to mitigate compliance risk from SI systems. — Be alert to instances when an SI system produces inaccurate or inconsistent outcomes, is used outside its intended purpose, or is not supported by controls that address applicable laws and regulations. — Implement controls that limit automated representations, require verification in higher-impact contexts, and support prompt correction and remediation.
Cybersecurity**	— Implement cybersecurity controls (e.g., identity and access management, data and model integrity, monitoring, incident response, and recovery) that extend to the SI lifecycle and supporting infrastructure. — Apply acceptable-use, privacy, and incident-reporting practices to agent identities, credentials, logs, and data use.

KPMG

© 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Pillar 4: Oversight *Establishes who monitors the SI system or agent and who is accountable for its use*

Component	SI-Specific Considerations to be Evaluated
Governance & Accountability	— Establish accountability for SI risk through defined roles and decision rights, risk appetite and autonomy exposure, validation, credible challenge, and timely board reporting. — Support governance with an inventory of approval authorities at meaningful lifecycle points.
Human-in-the-Loop & Human-on-the-Loop Controls**	— Define the nature and level of human oversight and human involvement calibrated to the potential consequences, autonomy, reversibility, and operating volume of the use case. — Demonstrate that the control operates as intended.
Performance Monitoring	— Calibrate metrics, thresholds, reporting, and escalation to a use case's potential consequences, autonomy, expected variability, and rate of change. — Monitor model performance after deployment to evaluate impact of changes to data, use patterns, prompts, permissions, providers, and underlying models.
Reporting & Transparency	— Conduct risk based internal reporting that includes material use cases, accountable owners, significant changes, control exceptions, incidents, customer remediation, concentrations, and assurance results. — Define internal escalation and notification thresholds. — Reconcile reports to the SI inventory, incident records, validation results, audit findings, and board reporting.

Pillar 5: Resilience *Addresses the bank's ability to detect, contain, recover from, and remediate SI system or agent failures while continuing critical business processes*

Component	SI-Specific Considerations to be Evaluated
Operational Resilience	— Develop a program to detect, contain, recover, remediate and continue business during either a loss of service or incorrect operation. — Consider internal SI systems, fallback processes, and external SI agents that interact through bank channels alongside scenario analysis that considers correlated or cascading activity across customers, agents, and providers.
Cybersecurity**	— Implement cybersecurity controls (e.g., identity and access management, data and model integrity, monitoring, incident response, and recovery) that extend to the SI lifecycle and supporting infrastructure. — Apply acceptable-use, privacy, and incident-reporting practices to agent identities, credentials, logs, and data use.

Pillar 6: Assurance *Provides evidence that SI system or agent controls continue to operate effectively*

Component	SI-Specific Considerations to be Evaluated
Testing	— Determine the appropriate range, rigor, frequency, and independence of testing based on the materiality of use cases, potential failure consequences, and limitations of the SI system. — Utilize testing over the SI lifecycle, including design and development, pre-deployment (e.g., testing "fit for purpose"), and post-deployment and use (e.g., testing for drift, control weaknesses). — Employ a variety of SI-specific testing approaches, such as subjective reviews, adversarial testing, red teaming, and "LLM-as-a-judge."
Documentation & Auditability	— Ensure that documentation is proportionate to each use case and addresses decision traceability, ownership, version and change control, prompts, permissions, approvals, and incidents, among others. — Assess whether the records might support reconstruction of material outputs or actions.
Third-Party & Vendor Risk	— Supplement existing third-party risk management practices with SI systems and vendor risk considerations for instances where the provider's SI can affect the bank's decisions, customers, or data. — Define the scope of authority and use, notification timelines (e.g., misfire, drift, manipulation), assigned responsibilities/liability, and processes for changes in SI functionality (e.g., new features, model changes).

KPMG

© 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Internal Audit & Independent Challenge	— Scale an audit framework tailored to the bank's SI use cases, including scope, cadence, skills, access, and reporting. — Provide independent assurance regarding governance, validation, control design, implementation, and the operation of the broader SI risk management framework.

Risk-Tiering. The OCC notes that the intensity of a bank's controls could increase with the potential consequences of an SI agent's failure or misuse. Higher consequence use cases may warrant greater restrictions on autonomy, stronger controls, more direct human oversight, more independent validation, or more robust resilience measures. Risk classification may be based on potential consequences, transfer of agency, and the degree of human oversight, rather than technical sophistication.

The OCC offers an illustrative "risk-tiering methodology" that could be applied to SI models and agentic systems, independent of business line, to scale expected controls based on risk. Under the methodology, a use case would be scored against a set of seven risk factors: decision consequence, reversibility, customer/financial impact, autonomy level, data sensitivity, explainability, and provenance, which would then be combined into a "composite tier" as follows:

Composite Tier	Example Profile Characteristics
Tier 1: Critical	— System takes direct action. — Low/no reversibility once action is executed. — High financial or customer impact/harm. — System functions autonomously or partially autonomous.
Tier 2: High	— System takes direct action or is a "high-weight" in support of a decision. — Human-on-the-loop monitoring with potential for intervention. — Moderate-to-high financial or customer impact/harm.
Tier 3: Moderate	— System provides support for a human decision. — Mandatory human-in-the-loop (i.e., approving the action). — Limited data sensitivity (e.g., whether inputs or outputs could constitute a privacy or consumer law exposure). — Output or action may be caught and undone (i.e., reversible).
Tier 4: Low	— No risk of customer/financial data exposure. — No direct action by the system. — System use fully human-controlled.

The supervisory framework also provides an appendix of terms, which the OCC considers a "living Lexicon." The definitions are expected to change as technology, use cases and supervisory understanding change and mature.

For more information, please contact:

David Anderson
Partner, Advisory
Offering Leader, Modeling, Credit and Liquidity
djanderson@kpmg.com

Katie Boswell
Managing Director, Advisory
US Lead, Trusted & Secure AI
katieboswell@kpmg.com

Kevin Lowery
Managing Director, Advisory
Banking, Regulatory & Compliance
klowery@kpmg.com

Mark Wickware
Managing Director, Advisory
Banking, Regulatory & Compliance
mwickware@kpmg.com

© 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.



Laura Byerly
Managing Director
Regulatory Insights
lbyerly@kpmg.com



Brian Hart
Principal
Risk, Regulatory and Compliance
bhart@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: **kpmg.com**

© 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.