

August 11, 2026

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or call your regular Skadden contact.

Monica Freas

Partner / Washington, D.C.
202.371.7100
monica.freas@skadden.com

Susanne Werry

Counsel / Frankfurt
49.69.74220.133
susanne.werry@skadden.com

David A. Simon

Partner / Washington, D.C.
202.371.7120
david.simon@skadden.com

This memorandum is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This memorandum is considered advertising under applicable state laws.

One Manhattan West
New York, NY 10001
212.735.3000

1440 New York Ave., NW
Washington, DC 20005
202.371.7000

TaunusTurm
Taunustor 1
60310 Frankfurt am Main
49.69.74220.0

The FSB's Sound Practices for Responsible AI Adoption: A Global Governance Framework for Financial Institutions

Executive Summary

- **What's new:** The Financial Stability Board published a consultation report distilling AI governance observations into 12 nonbinding "sound practices" covering the full AI life cycle for financial institutions.
 - **Why it matters:** The recommended practices consolidate governance expectations emerging across major financial regulators and are likely to influence supervisory practice, affecting multinational financial institutions operating across jurisdictions.
 - **What to do next:** Financial institutions should consider benchmarking current governance framework against the FSB framework, maintaining a centralized AI inventory and strengthening third-party risk management. We translate the 12 practices and provide an annex of case studies.
-

In June 2026, the Financial Stability Board (FSB) published its consultation report, "Sound Practices for Responsible Adoption of Artificial Intelligence (AI)." Rather than creating new international standards, the report distills governance practices already emerging across leading financial institutions into twelve nonbinding recommended practices covering the full AI life cycle.

The report is notable for its practical focus. Drawing on case studies from banks and insurers, it illustrates (i) how institutions are deploying AI in production, (ii) the governance challenges they have encountered and (iii) the controls they have implemented. Rather than prescribing particular technologies, the report focuses on governance, accountability, documentation and life-cycle risk management.

Key Features and Opportunities

- Although nonbinding, the FSB's 12 sound practices consolidate the governance expectations emerging across major financial regulators and are likely to influence supervisory practice.
- The report reinforces that AI governance should be integrated into existing governance, operational risk and compliance frameworks — not managed as a stand-alone technology initiative.
- The FSB's recommendations closely mirror the direction of AI regulation and governance across major jurisdictions.
 - In the European Union, the recommendations align with governance concepts embedded in the EU AI Act and the Digital Operational Resilience Act (DORA),

The FSB’s Sound Practices for Responsible AI Adoption: A Global Governance Framework for Financial Institutions

- including board oversight, documentation, human oversight, data governance and third-party risk management.
- In the United States, the recommendations complement existing supervisory focus on governance, risk management, explainability, data privacy, third-party risk, cybersecurity and consumer protection.
- Financial institutions can use the framework to benchmark governance now, particularly for material, customer-facing and third-party AI deployments.

The report is significant because it consolidates supervisory thinking into a coherent governance framework. For

multinational financial institutions, the FSB framework provides a practical operating model that can be used as a common global baseline while accommodating jurisdiction-specific legal requirements. Firms that already have mature governance, operational resilience and third-party risk programs will often be able to extend those frameworks to AI rather than creating entirely new governance structures.

How to Use the 12 Sound Practices

The 12 sound practices are best understood as concrete governance actions to guide sound enterprise-wide implementation.

FSB Sound Practice	Practical Implication
1. Strategic direction	Adopt a board-approved AI strategy and define AI risk appetite.
2. Governance	Allocate clear accountability roles and responsibilities across business, technology, legal, compliance, risk and audit functions.
3. AI risk management	Integrate AI into enterprise risk management using inventories, approvals and life-cycle documentation.
4. Organizational adaptability	Review governance periodically as AI capabilities and regulation evolve; adapt and adjust oversight accordingly.
5. Materiality	Apply a systematic approach to assess the materiality and risk of AI use cases at the inception stage and thereafter. Rank AI use cases according to risk and apply proportionate controls.
6. Model selection	Evaluate AI solutions against business objectives, explainability and operational resilience.
7. Data governance	Ensure data is fit-for-purpose for training, testing and using AI (i.e., accurate, complete, consistent, reliable, secure). Strengthen controls over data quality, lineage, privacy and security.
8. Explainability and transparency	Use explainable AI where appropriate or implement compensating controls. Provide appropriate transparency tailored to different stakeholders.
9. Performance management	Continuously validate, monitor and test AI systems with performance assessments.
10. Human oversight	Implement effective human oversight considering the materiality, risk, autonomy, complexity and explainability of different AI use cases. Define mandatory review and override points for material decisions.
11. Cyber resilience and ICT risk management	Include AI and evaluate information and communications technology (ICT) within cybersecurity testing and operational resilience programs.
12. Third-party AI risk management	Expand vendor due diligence, contractual protections, monitoring and exit planning. (Consider performance, transparency, data quality, supply chain and concentration risks, and business continuity.)

The FSB's Sound Practices for Responsible AI Adoption: A Global Governance Framework for Financial Institutions

What the FSB Case Studies Demonstrate

The case studies consistently show that institutions are realizing substantial productivity gains from AI, but only where governance matures alongside deployment. Four themes emerge:

- Successful AI deployments retain meaningful human oversight for material or customer-facing decisions.
- Enterprise AI inventories and centralized governance become increasingly important as AI adoption scales.
- Continuous testing, monitoring and documentation are essential to maintain performance over time.
- Third-party AI introduces distinct transparency, accountability and concentration risks that require enhanced vendor governance.

See our Annex: [Case Studies From the FSB Report — What Worked and What Needed Refinement](#) for examples and details.

Practical Takeaways

- The FSB framework reinforces the emerging global consensus that regulators expect AI governance to be embedded within existing enterprise risk, compliance, operational resilience, cybersecurity and third-party risk management frameworks — not managed as a stand-alone AI program.
- The guidance illustrates increasing convergence among major regulatory regimes, including the EU AI Act, DORA, U.S. financial regulators' AI governance and risk-management expectations, and supervisory guidance emerging in

jurisdictions such as the U.K., Singapore and Japan. This is particularly relevant for multinational financial institutions seeking a common global governance baseline.

- The emphasis on inventories, life-cycle governance, human oversight, documentation and third-party risk reflects themes that are appearing consistently across AI regulation and supervisory guidance worldwide, suggesting these capabilities are becoming core governance expectations regardless of jurisdiction.
- Notably for boards and company management, many institutions can likely leverage existing governance investments — including operational resilience, model risk management, cybersecurity, vendor management and compliance functions — rather than creating entirely new AI governance structures.

The FSB's consultation on the sound practices has now closed, and the FSB is expected to consider stakeholder feedback before finalizing the guidance. Firms should monitor whether the final guidance differs in any material respects from the consultation version.

Meanwhile, although the recommended practices remain nonbinding, the consultation underscores the FSB's continued focus on promoting consistent approaches to AI governance across the global financial sector. Financial institutions should therefore continue to monitor developments and assess whether their existing AI governance frameworks align with the governance expectations reflected in the report. We will continue to monitor developments and provide updates as the FSB progresses [this initiative](#).

The FSB’s Sound Practices for Responsible AI Adoption: A Global Governance Framework for Financial Institutions

Annex: Case Studies From the FSB Report — What Worked and What Needed Refinement

Use Case	What Firms Are Doing
Credit Underwriting	A midsize bank applied generative AI to create credit narratives, reducing drafting time for a preliminary proposal from over a day to 15 minutes, but the tool achieved only approximately 80% accuracy in financial data extraction. With roughly one in five extractions still requiring correction, this use demonstrates that even successful generative AI credit tools need ongoing human review.
Fraud Detection (Transactions)	A large internationally active bank built an in-house agentic AI system that monitored more than 80 million daily signals across transactions, card payments and digital banking interactions to detect emerging fraud and scam patterns and autonomously propose new detection rules for human review before implementation. The system now drives 75% of the bank’s card fraud rules and helped reduce fraud losses by more than 20% in the first half of the 2026 financial year versus the same period in 2025.
Fraud Detection (Identity)	A digital bank enhanced its facial recognition tool to also detect suspicious image backgrounds by combining facial feature matching with background analysis. This new capability helped identify mule account controllers and strengthens detection of account takeover, deepfakes and fake-identity loan applications, completing comparisons in seconds.
Operational Efficiency	A large internationally active insurer conducted a global review of manual workflows and eliminated roughly 400,000 instances of manual processing in 2025 through AI adoption. The insurer’s highest-impact example automated the underwriting “quick quote” process, reducing turnaround from (i) one to three business days to (ii) about 45 seconds. The insurer also deployed AI code-generation tools company-wide, producing six million lines of code in 2025 with an 80% developer adoption rate.
Developmental Testing	A large bank built a new machine-learning trading model expecting it to outperform the bank’s existing non-AI model. Testing showed the new model (i) did not consistently outperform the old one, (ii) did not produce training data representative of live production data, and (iii) was harder to evaluate due to its added complexity, so the bank postponed deployment of the AI model and kept using its existing non-AI model.
Third-Party Risk Management	Banks have encountered recurring challenges with third-party AI systems, including “information gaps” (limited visibility into vendors’ training data, model details or how the vendor uses the bank’s own data) and “accountability gaps” (where the bank remains legally accountable for AI outcomes even when it did not build the tool in-house). Any firm relying on third-party AI tools will face these structural problems and may need to adjust third-party risk management frameworks accordingly.

The FSB’s Sound Practices for Responsible AI Adoption: A Global Governance Framework for Financial Institutions

Use Case	What Firms Are Doing
Relationship Management	A global systemically important bank (G-SIB) piloted an integrated AI platform to help the bank’s corporate relationship managers, who had faced time pressure synthesizing information and preparing tailored client proposals, leaving some clients underserved. The platform integrated external sources such as news feeds and research reports with internal knowledge bases to help generate insights and draft proposals. This reduced preparation time by roughly 50%, enabled three times more client dialogue and allowed managers to serve previously underserved clients.
Accurate Documentation	Several large internationally active banks started maintaining a centralized, organization-wide AI inventory supported by dedicated software systems, giving the banks clear visibility into their AI footprint and associated risks. These systems documented each AI use case throughout its life cycle, capturing attributes such as purpose, scope of use, risk materiality rating and responsible personnel. The systems also supported automated tracking of approvals and issues, helped identify inter-dependencies between models and tracked life cycles with checkpoints at key risk management stages.
Aligning Capabilities With Strategy	Some large financial groups started redesigning processes end-to-end and investing in capability building through leadership master classes, staff AI bootcamps and organization-wide AI literacy programs. The firms set targets to track AI adoption progress, but acknowledged that finding suitable metrics remained challenging, particularly for value realization. Other institutions tried a narrower approach, layering AI onto existing processes and restricting staff to specified tools within prescribed platforms, without pursuing broader implementation.
Adaptive AI Strategy	A G-SIB’s AI approach evolved through adaptive governance and controls as AI became embedded in core business infrastructure. As adoption expanded over time, the bank identified that its decentralized development had become a limitation, prompting the bank to restructure by creating a centralized AI group reporting directly to the CEO. The group prioritizes use cases; coordinates deployment across business lines; and standardizes risk, security and compliance practices.

Summer associate **Grace Shuette** contributed to this article.