Deloitte.

US Department of Treasury announces public-private initiative aimed at strengthening cybersecurity and risk management for AI

Initial perspectives on AI risk management, governance, and controls for financial services

Center *for* **Regulatory Strategy US**

On February 18, 2026, the US Department of the Treasury announced the conclusion of a major public-private initiative to strengthen cybersecurity and risk management for artificial intelligence (AI) in the financial services sector.[1] The Artificial Intelligence Executive Oversight Group (AIEOG) developed practical resources covering data, governance, fraud, transparency, and digital identity to help institutions adopt and deploy AI. The approach is implementation-focused and aims to strengthen the security of AI data, infrastructure, and models while promoting global adoption of American AI systems in support of the president's AI Action Plan.[2] The workstreams cover the following areas: AI Lexicon and Taxonomy, Financial Services AI Risk Management Framework (FS AI RMF), Explainability, Data-Nutrition Labeling, AI-enhanced Fraud, and Identity and Authentication.[3]

5 insights you should know

Enabling consistent AI terminology across financial services: The AI Lexicon develops a shared AI terminology to support clearer discussion of AI risk and technical topics.[4] It aggregates definitions from established standards and public sources, such as National Institute of Standards and Technology (NIST) and federal and international financial regulators, to help reduce ambiguity in interpreting AI-related terms.

Structured AI risk management framework and sector-specific actionable controls: The FS AI RMF turns broad AI principles into practical, financial services-specific control objectives and implementation guidance.[5] Designed to align with the NIST AI Risk Management Framework (AI RMF), it intends to provide a consistent way for institutions and their value chains to assess, benchmark, and measure the maturity of their own governance around AI. With 230+ actionable control objectives, it helps organizations evaluate their current stage of AI adoption, tailor controls to their risk profile, and embed AI risk management into existing enterprise governance.

Assessment of AI maturity through staged adoption and risk-based evaluation: The AI Adoption Stage Questionnaire (ASQ) offers a standardized self-assessment to help institutions identify their current AI maturity across four levels: Initial, Minimal, Evolving, and Embedded.[6] It uses business impact, technology implementation, and scalability to provide a risk-aligned view of AI deployment. By assessing areas such as governance, deployment approaches, third-party use, and data criticality, organizations may better benchmark and build a phased roadmap toward scalable, enterprise-wide AI adoption.

Operationalizing AI risk management through a comprehensive control framework: The Risk & Control Matrix (RCM) is a structured, NIST AI RMF-aligned set of control objectives to help organizations assess, prioritize, and implement AI risk management practices.[7] It is organized around four core functions: Govern, Map, Measure, and Manage, which translates AI risks into practical categories and sub-categories. The supporting Guidebook and Control Objective Reference Guide are intended to help turn the framework into practical implementation, methodically prioritize controls, integrate risk mitigation into daily operations, and expand governance as AI matures.

AI-driven identity and authentication risks: The Financial Services Sector Coordinating Council's (FSSCC) AI and Identity and Authentication Workstream (AI-IA) stresses that GenAI is transforming identity and authentication risks, enabling attacks such as deepfake impersonation and synthetic identity fraud.[8] The caveats in traditional digital controls (e.g., identity verification methods) should be transitioned to adaptive defenses like behavioral biometrics and phishing-resistant authentication, encouraging institutions to use a "fight AI using AI" strategy to build resilient identity ecosystems.

5 considerations to evaluate

1 **Define AI scope and taxonomy:** Financial institutions should establish a clear definition of "in-scope AI" and AI taxonomy aligned with industry standards to address the inconsistencies in technical and risk management terminology that may hinder effective governance, oversight, and adoption of AI. Further, organizations should consider maintaining a centralized inventory of AI use cases to encourage an enterprise-wide, consistent use of AI.

2 **Organizations to expect increased regulatory focus on AI risk management governance and controls**: The FS AI RMF may increasingly serve as a reference framework for regulators, auditors, boards, and risk committees. Accordingly, financial institutions should begin assessing gaps in current AI governance and controls against the FS AI RMF, establishing and maintaining an enterprise AI inventory, and updating third-party due diligence and contracting standards to address AI-specific risks, control requirements, and audit evidence expectations.

3 **Structured implementation path and not just a compliance checklist:** The AI ASQ can act as the first phase in the AI adoption roadmap, helping organizations classify their AI maturity. The ASQ can be positioned as a baseline to determine each AI use case's maturity stage to ensure that oversight is proportional to risk and operational reality. The assessment also enables comparability and benchmarking across levels of maturity, highlights the specific capability gaps blocking safe production, and can support a phased roadmap.

4 **Design controls that are testable and evidence-backed:** Financial institutions should translate FS AI RMF control objectives into measurable terms (e.g., validation frequency, monitoring thresholds, documentation standards) and these should be linked to evidence that can be consistently produced. Firms should keep their evidence expectations practical, repeatable, and embedded into delivery and operational workflows to avoid ad-hoc compliance efforts. Testing and issue management processes should be defined to support sustained assurance.

5 **Design dynamic risk-based identity systems by strengthening industry collaboration and intelligence sharing:** Financial institutions should treat AI-driven identity risk as a structural shift requiring intelligence-led identity frameworks. This may require embedding AI governance and model risk controls with enhanced operational readiness through updated processes, training, and incident response mechanisms for AI-enabled threats. An integrated framework together with identity, defense, fraud, cybersecurity, and governance functions is a leading way to proactively detect, prevent, and respond to AI-powered attacks.

Endnotes

1. US Department of Treasury press release, "Treasury Announces Public-Private Initiative to Strengthen Cybersecurity and Risk Management for AI," February 18, 2026.
2. The White House, "Winning the Race: America's AI Action Plan," July 2025.
3. Financial Services Sector Coordinating Council (FSSCC), "Financial Sector Artificial Intelligence Executive Oversight Group Deliverables," accessed March 27, 2026.
4. FSSCC, "Artificial Intelligence Executive Oversight Group AI Lexicon - February 2026," February 18, 2026.
5. Cyber Risk Institute, "Financial Services AI Risk Management Framework," accessed March 27, 2026.
6. Cyber Risk Institute, "AI Adoption Stage Questionnaire," accessed March 27, 2026.
7. Cyber Risk Institute, "Risk and Control Matrix (RCM)," accessed March 27, 2026.
8. FSSCC, "Artificial Intelligence Executive Oversight Group AI Lexicon - February 2026," February 18, 2026.

Connect with us

Clifford Goss
Partner
Deloitte & Touche LLP
cgoss@deloitte.com

Gowri Zoolagud
Managing Director
Deloitte & Touche LLP
gzoolagud@deloitte.com

Kirat Dhillon
Senior Manager
Deloitte & Touche Assurance and Enterprise Risk Services India Private Limited
kidhillon@deloitte.com

Palak Kaur
Senior Consultant
Deloitte & Touche LLP
palkaur@deloitte.com

Khushboo Bansal
Consultant
Deloitte & Touche Assurance and Enterprise Risk Services India Private Limited
khusbansal@deloitte.com

Deloitte Center for Regulatory Strategy, US

Irena Gecas-McCarthy
FSI Director, Deloitte Center for Regulatory Strategy, US
Principal
Deloitte & Touche LLP
igecasmccarthy@deloitte.com

Aaron Salerno
Manager
Deloitte Services LP
asalerno@deloitte.com

Kyle Cooke
Manager
Deloitte Services LP
kycooke@deloitte.com