Deloitte.

'Weapon and tool' - systemic risk implications of AI in banking and finance

Initial perspectives related to remarks by the Acting Comptroller of the Currency, Michael J. Hsu

Center *for* Regulatory Strategy US

On June 6, 2024, Acting Comptroller of the Currency Michael J. Hsu delivered remarks at the Conference on Artificial Intelligence and Financial Stability, hosted by the Financial Stability Oversight Council (FSOC) in partnership with the Brookings Institution, wherein he discussed systemic risk implications of artificial intelligence (AI) and offered his thoughts on approaches to AI deployment to improve its safety.[1] His remarks are the latest illustration of regulators' growing concern about AI. In its *2023 Annual Report*, FSOC—for the first time—identified AI as a potential systemic risk.[2]

5 insights you should know

AI presents accountability challenges: AI's ability to evolve overtime and self-learn makes it a powerful tool but can also result in model drift, where the model's accuracy and performance deviate from expectations. This may be especially true in the case of nontransparent models that are powered by third parties. Banks may struggle to identify whom to hold accountable for what or how to fix any issues, which could—ultimately—erode trust within the banking system.

Competitive pressures may cause banks to neglect controls: As competitive pressures grow within the industry to develop and launch AI-enabled applications, risk management and controls may be neglected by some banking organizations. As a result, risks may grow undetected and unaddressed until a critical failure or disruption occurs. It is therefore critically important for adequate initial due diligence, and risk management and controls to keep pace with growth in order to drive sustainable growth and stability.

AI-enabled fraud is a top concern: Nefarious actors are increasingly able to access and deploy AI-enabled tools for fraudulent activities. For example, AI tools—including deepfakes—may be used to impersonate an individual's voice or likeness to trick friends and family to send money to a fraudster or even bypass a bank customer's account security check. AI may be used to drive the increase in the scale and scope of fraud, which could undermine trust in the payments and banking system.

AI-enabled cyberattacks are a growing risk: Cybercriminals are increasingly deploying AI-enabled tools to launch sophisticated attacks on individuals and organizations. The frequency and scale of cybercrime, such as ransomware attacks, may increase. These tools are not only being used by criminal organizations, but also nation-state actors to disrupt or disable critical infrastructure. It is therefore important for both policymakers and banking organizations to focus on operational resilience.

Shared responsibility model for AI: The Acting Comptroller proposed a shared responsibility framework for AI, similar to that used in the cloud computing context, where responsibilities of customers and AI-technology service providers are allocated depending upon the "AI stack" layer and service arrangement. One potential vehicle for facilitating this framework could be the newly established US Artificial Intelligence Safety Institute (AISI) within the National Institute of Standards and Technology (NIST).

5 considerations to evaluate

1 **Establish clear roles and responsibility:** Banks should apply existing principles of risk governance and model risk management (see Federal Reserve Supervisory Letter 11-7, OCC Bulletin 11-12, and the *Comptroller's Handbook* on Model Risk Management)[3] to their AI applications and across their model lifecycles. For third-party AI-tools that may pose particular challenges to an organization's internal accountability framework, controls should be put in place commensurate with the bank's risk exposure and complexity and extent of the model's usage.

2 **Develop gates between AI development stages:** Banks should identify in advance "gates" or points at which pauses in growth and development are needed to establish controls as AI develops across the maturity spectrum. Hsu stated AI applications evolve across three stages: (1) *inputs* where AI provides information for humans to act upon; (2) *co-pilots* where AI enables humans to do tasks more quickly; and (3) *agents* where AI executes activities on behalf of humans. It's important for banks to demonstrate to regulators a coherent AI strategy with controls.

3 **Invest in customer protection and compliance:** Leveling up customer security protocols and consumer compliance should be considered, so as to better align with evolving AI technologies. This may include investing in AI-enabled security solutions to detect and respond to AI-fraudulent activities in real-time, such as advanced behavioral analysis and anomaly detection. Additionally, banks should proactively manage the risk of consumer compliance violations, such as prioritizing model accountability and transparency particularly for consumer-facing applications.

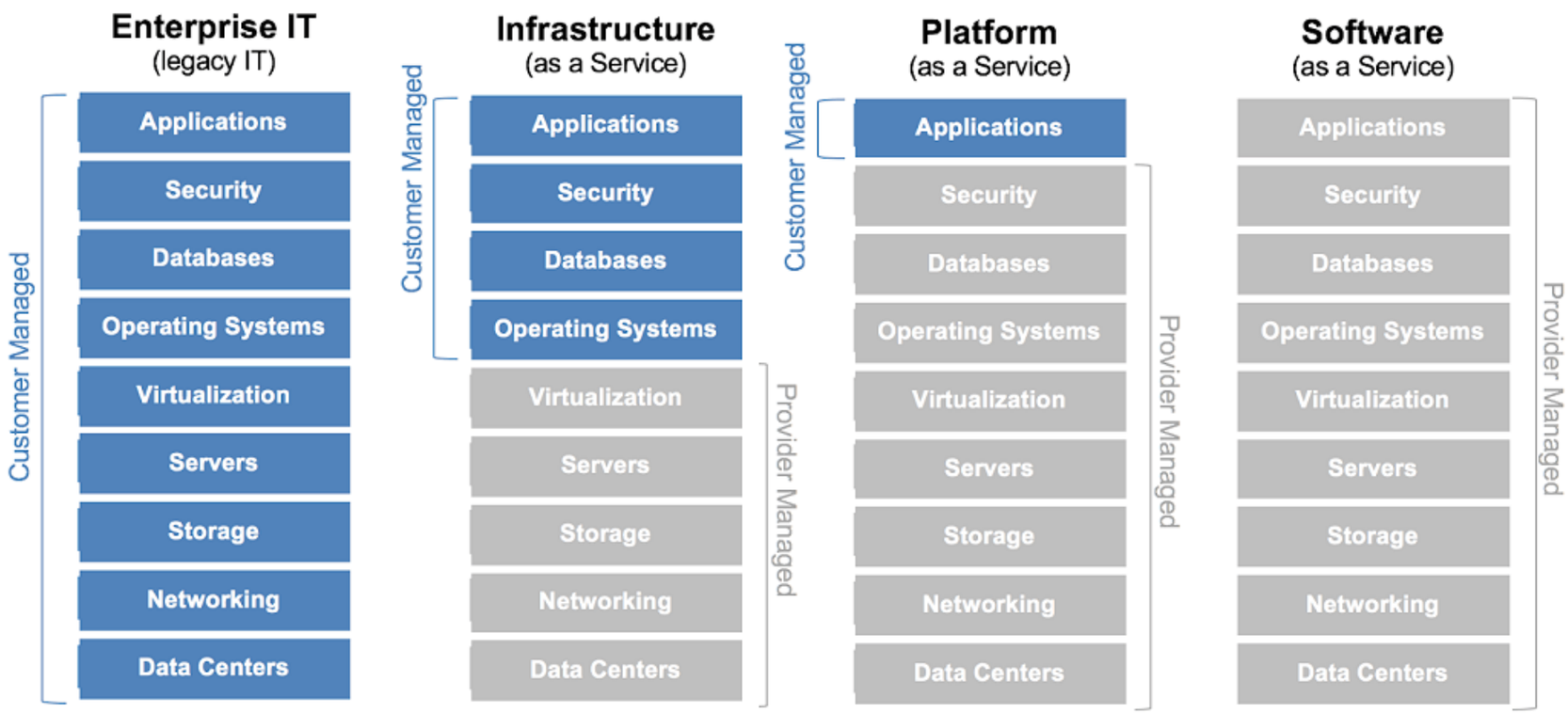
4 **Invest in cybersecurity and operational resilience:** Strategic attention should be given to evaluating cybersecurity defenses, including technology infrastructure and endpoint detection and response (EDR) solutions, to assess their suitability against potential AI threat actors. Building resilient organizations involves not only building leading technology systems, but also maintaining disaster recovery and business continuity plans that are regularly updated and tested to ensure they are effective against AI-enabled threats.

5 **Engage with industry and public-private collaboration initiatives:** Consider engaging with regulator-convened forums, such as NIST's AI Safety Institute Consortium and other collaboration efforts such as industry member groups. Coordination among and in between industry participants and policymakers will likely be key to developing AI standards, including a potential shared responsibility framework. Participation can also help share knowledge and leading practices between AI stakeholders and improve both the industry and banks' AI practices.

Acting Comptroller Hsu proposed a "shared responsibility framework" similar to what exists in the cloud computing context, which allocates operations, maintenance, and security responsibilities to customers and cloud service providers depending on the service a customer selects. See Figure 1 below.

Within the "AI stack," there exists (i) an infrastructure layer, (ii) a model layer, and (iii) an application layer. But, according to Acting Comptroller Hsu, for the framework to be actionable, consensus on the sub-components within each layer and on the types of third-party arrangements would be needed—something FSOC is uniquely positioned to contribute to, given its role and ability to coordinate among agencies, organize research, seek industry feedback, and make recommendations to Congress.

Figure 1: Shared responsibility model in cloud computing



Source: General Services Administration (GSA), "Cloud Information Center," accessed June 10, 2024.

Deloitte.

Endnotes

[1] Office of the Comptroller of the Currency (OCC), "Acting Comptroller of the Currency Michael J. Hsu remarks 'AI Tools, Weapons, and Accountability: A Financial Stability Perspective,'" June 6, 2024.

[2] Financial Stability Oversight Council (FSOC), "Annual Report 2023,'" December 2023.

[3] Federal Reserve Board of Governors (FRB), "SR 11-7: Guidance on Model Risk Management," April 4, 2011; OCC, "Bulletin 11-12: Supervisory Guidance on Model Risk Management," April 4, 2011; OCC, "Comptroller's Handbook on Model Risk Management," August 2021.

Connect with us

Richard Rosenthal
Principal
Deloitte & Touche LLP
rirosenthal@deloitte.com

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

John Graetz
Principal
Deloitte & Touche LLP
jgraetz@deloitte.com

Satish Lalchand
Principal
Deloitte Transactions and Business Analytics LLP
slalchand@deloitte.com

Paul Sanford
Independent Senior Advisor to Deloitte & Touche LLP
pasanford@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