

FARO

REPORT

BANKING · INSURANCE · WEEKLY ANALYSIS



Key Trends in the Insurance Sector This Week

S24-2026-INS · Reporting Period: June 8-15, 2026

NAIC AI Evaluation Tool Enters Active Examination Phase. The NAIC's AI Systems Evaluation Tool is now in a 12-state pilot (March–September 2026) covering CA, CO, CT, FL, IA, LA, MD, PA, RI, VT, VA, and WI, with formal adoption expected at the Fall 2026 National Meeting. The tool provides a standardized framework to assess AI governance, high-risk models, data inputs, and third-party vendors during examinations. The pilot converts principle-based guidance into structured examination questions.

Hurricane Season 2026: Below-Average Forecast Does Not Reduce Underwriting Exposure. NOAA forecasts below-normal Atlantic activity for the first time since 2015. Allianz Commercial notes that storm counts remain a poor proxy for insured losses.

Munich Re RiskScan 2026: AI, Cyber, and Catastrophe Emerge as Systemic Convergence. Munich Re's RiskScan 2026, a survey of US and UK insurance professionals and consumers, found AI ranked as the single most impactful risk facing the industry, with cyber threats and natural catastrophes in the top three. Munich Re US CEO Marcus Winter noted that risks are increasingly systemic rather than isolated, driven by the interconnected nature of digital exposure, supply-chain dependencies, and climate-driven event severity. Protection gaps for both flood and cyber coverage remain persistent among businesses. The survey signals a structural shift: the traditional separation of technology risk, financial risk, and catastrophe risk is collapsing into a single systemic exposure frame.

AI Cyber Coverage Repriced as Mythos Access Expands to 150 Organizations. Anthropic expanded access to its Mythos cybersecurity model, previously limited to a handful of large technology and Wall Street firms, to 150 additional organizations. The NYDFS had issued an advisory on May 21 warning regulated entities that frontier AI models amplify the speed and scale at which threat actors can identify vulnerabilities. For cyber insurers, the Mythos expansion has a dual effect: it raises the offensive threat baseline (more sophisticated attacks available to more actors) while also expanding defensive AI capability. Underwriters are reassessing pricing models for cyber policies where AI-enabled attacks compress response windows and raise potential severity.

Affirmative AI Coverage Crystallizes as the Structural Answer to Silent Exposure. The insurance market is reaching a structural inflection: ISO exclusions effective January 2026 removed AI-related bodily injury and property damage from standard CGL policies, forcing a clear separation between silent and affirmative AI coverage. Dedicated AI liability products from Testudo, Coalition, AXA XL, Hiscox, and Beazley are filling the gap at limits of \$2–\$50 million. A Gallagher survey of 1,250 companies found 57% identify AI errors, hallucinations, and misinformation as their top risk. The unresolved challenge is liability allocation between AI vendors and deploying enterprises.

MY TAKE

The convergence of NAIC examination activity, hurricane season onset, and the Mythos expansion makes this week a meaningful calibration point for the sector. Carriers face three simultaneous pressures: regulatory documentation requirements arriving through market conduct examinations, catastrophe underwriting discipline that cannot relax regardless of seasonal forecasts, and a cyber threat landscape being reset by the broadening of frontier AI access. The affirmative AI coverage market is the most commercially dynamic area, but it is being built in real time without loss history, actuarial precedent, or settled liability doctrine.

TECH TERM OF THE WEEK: "Foundation Model Risk"

The risk that a failure, vulnerability, or unexpected behavior in a widely adopted foundation model generates simultaneous impacts across multiple organizations that depend on it. Because many AI applications rely on a few shared models, a single model-level event can create correlated operational, financial, cyber, and liability losses across industries and geographies. This concentration makes foundation model risk a growing concern for insurers, reinsurers, regulators, and financial institutions.

FARO

REPORT

BANKING · INSURANCE · WEEKLY ANALYSIS



Key Trends in Core Banking This Week

S24-2026-BNK · Reporting Period: June 8-15, 2026

OCC and Fed Begin Active AI Examination of Banks. Reuters reported on June 12 that supervisors from the Office of the Comptroller of the Currency and the Federal Reserve have begun asking detailed questions about AI during routine bank examinations. Questions focus on governance, oversight, vendor management, subcontractor visibility, and contingency planning. The shift is structural: AI is no longer being reviewed as an innovation initiative but as an operational risk category within the standard safety-and-soundness examination framework. Banks without formalized AI governance documentation and model inventories, vendor contracts, and escalation procedures, are now facing examination exposure, not future regulatory risk.

Third-Party AI Risk: The Examination Perimeter Extends Beyond the Bank's Systems. OCC examinations now extend to subcontractors and fourth-party providers. Banks using third-party AI for credit decisioning, fraud detection, or compliance are being asked to demonstrate visibility into their providers' governance, model documentation, and failure contingency plans. The principle emerging from examiner conversations is unambiguous: outsourcing AI does not outsource accountability. Cambridge CCAF reports fintechs lead incumbents 47% to 30% in advanced AI adoption, while oversight of third-party AI relationships remains limited.

Colorado AI Act Enforcement Begins June 30: Days Remaining, Not Quarters. Colorado's AI Act (SB†24-205) takes effect June 30, 2026, requiring high-risk AI systems, including credit-scoring tools, to implement risk management, impact assessments, and transparency controls. Penalties reach \$20,000 per violation, or \$50,000 where senior citizens are affected. No comprehensive federal banking AI standard currently satisfies the Act's safe-harbor provision.

Cambridge CCAF Report: Fintechs Lead Incumbents; Regulators Trail Both. The 2026 Global AI in Financial Services Report from the Cambridge Centre for Alternative Finance surveyed firms and regulators across multiple jurisdictions. Key findings: 81% of financial services firms are adopting AI at some level; fintechs report advanced adoption (scaling or transforming) at 47% versus 30% for incumbents. Only 20% of regulators report advanced AI adoption. 78% of regulators expect AI to become significant or transformative by 2030 despite limited internal adoption. 24% of industry respondents expect a net reduction in workforce roles; reskilling is the dominant expectation rather than displacement.

Revolut Co-Founder and CTO Steps Down: Governance Transition at Europe's Largest Neobank. Vlad Yatsenko, CTO and co-founder of Revolut, has stepped down. Yatsenko co-built Revolut's core technology infrastructure since the firm's founding in 2015; the platform now serves over 50 million customers. The departure follows Revolut's transition into a fully licensed banking institution.

MY TAKE

The June 12 Reuters report on OCC and Fed AI examinations is the most consequential development of the week for banking practitioners. It removes ambiguity: AI governance is not a future compliance requirement. It is a present examination matter. Banks without model inventories, vendor oversight, and kill-switch procedures are behind on examination readiness. The Colorado deadline on June 30 adds a state-level enforcement layer that will arrive before most institutions have resolved their federal posture.

TECH TERM OF THE WEEK: "Model Inventory"

A centralized registry of all AI and machine learning models deployed by a financial institution, including their purpose, ownership, validation status, and governance documentation. Regulators increasingly view model inventories as a foundational control for identifying model risk, third-party dependencies, and governance gaps.