



Our Take

PwC's Financial Services Risk & Regulation Update

9.18.26 Topics: TPRM | Clarity | FDIC | NYDFS | AML | On our radar

1 Agencies propose more flexible third-party risk management guidance

What happened? On September 11th, the Fed, OCC, FDIC, and NCUA proposed new [interagency third-party risk management \(TPRM\) guidance](#). It would replace the [current interagency guidance](#) issued in 2023.

How would the proposed guidance change current expectations? The proposal retains the principle that banks are responsible for risks arising from third-party relationships, but significantly revises expectations for how those risks are identified, assessed, and managed. As supervisory guidance, it also states that deviation from its examples or an examiner's view of best practices would not, by itself, provide a basis for supervisory action and that "the agencies will give due consideration to a banking organization's reasonable decisions in matters of third-party risk management supervision." Key changes include:

- **Risk identification and assessment.** Unlike the 2023 guidance, which is organized around the third-party relationship life cycle, the proposed guidance places risk identification and assessment at the center of the framework. It states that banks can assess third-party relationships based on the likelihood and potential magnitude of harm and use those assessments to determine the appropriate level of oversight.
- **Tailoring.** The proposed guidance places greater emphasis on tailoring risk management practices to a bank's size, complexity, risk profile, and the nature of individual third-party relationships. The proposal also includes examples intended to support more streamlined approaches for smaller institutions, including scaled due diligence, reliance on external information sources, shared risk management resources, and less extensive inventories for lower-risk relationships.
- **Residual risk acceptance.** The proposed guidance establishes residual risk acceptance as a standalone component of the framework, which was not included as a separate component in the 2023 guidance. It states that banks are not expected to eliminate all third-party risk and may accept residual risks that remain within their risk appetite and tolerances.
- **Higher-risk relationships and criticality.** The proposed guidance removes "critical activities" as a distinct category for determining the appropriate level of oversight and instead focuses on the likelihood and potential magnitude of harm presented by each relationship. It also states that certain characteristics, such as third-party access to systems or networks, do not automatically indicate a higher-risk relationship.
- **Due diligence.** The proposed guidance states that banks can scale due diligence activities according to risk and acknowledges that relevant information may not always be available, including when a third party is unable or unwilling to provide it or has a limited operating history. To address this, it states that banks can use public information, trade associations, external experts, co-ventures, consortia, certification organizations, consultants, auditors, and shared due diligence arrangements to support their assessments.

- **Affiliate relationships.** The proposed guidance recognizes that affiliated service providers may present lower risks than unrelated providers. It also states that banks may consider a third party's existing regulatory obligations and oversight as part of the risk assessment, while emphasizing that regulated entity status alone is not a substitute for effective TPRM.
- **Contract negotiation.** Unlike the 2023 guidance, which provided a lengthy list of contractual considerations, the proposed guidance states that there are no generally applicable expected contract terms. It recognizes that standard-form contracts may be appropriate in some circumstances, that banks may focus negotiations on the provisions most relevant to the risks presented by the relationship, and that limited negotiating leverage need not preclude a bank from proceeding when residual risks remain within its risk appetite and tolerances.
- **Ongoing monitoring.** The proposed guidance allows banks to tailor monitoring activities based on risk and changing circumstances. Unlike the 2023 guidance, which emphasized maintaining a complete inventory of third-party relationships and described a broad range of potential monitoring activities, the proposal also recognizes that extensive inventories and monitoring practices may not be necessary for certain lower-risk relationships.
- **Operational resilience.** The proposed guidance integrates operational resilience considerations into the risk-assessment process, including factors such as recovery capabilities, alternative providers, and the ability to resume operations following disruption.
- **Relationship termination.** The proposed guidance recognizes that decisions regarding third-party relationships may consider practical factors, including the costs and benefits of termination, the availability of alternatives, transition complexity, and the bank's broader assessment of risk.
- **Governance.** Relative to the 2023 guidance, the proposed guidance provides fewer prescriptive governance expectations and emphasizes structuring governance and board reporting according to the institution's size, complexity, risk profile, and third-party relationships, while continuing to recommend clear roles and responsibilities, risk appetite, reporting, documentation, and independent review.

What's next? Comments on the proposal are due by November 16th. The agencies are specifically seeking comment on whether the guidance should apply only to third-party relationships governed by written agreements and whether the final guidance should identify characteristics that generally indicate a higher-risk relationship.



Our Take

TPRM joins the broader shift toward individual firm risk judgment and accountability

The proposed updates to TPRM guidance are the latest initiative to advance current agency leadership's preference for greater tailoring, reduced prescriptiveness, and increased reliance on banks' own judgment. One of the most significant shifts is the elevation of risk identification and assessment as the primary determinant of how much oversight a third-party relationship receives instead of uniform standards. This will grant banks more latitude to determine where oversight resources are most appropriately deployed, while increasing the importance of the risk-rating methodologies, criticality frameworks, and risk appetite statements used to support those decisions. The challenge will be making sure that those methodologies are understandable, explainable, and defensible. Many institutions' third-party risk assessment approaches have become increasingly complex over time, often combining criticality determinations, inherent and residual risk measures, control assessments, concentration considerations, and other factors into classifications that can make it difficult for oversight functions, management, and boards, to clearly understand how a relationship's risk profile translates into contracting decisions and appropriate oversight.

The proposal also reflects another theme evident in the agencies' recent work: that effective risk management does not require the elimination of all risk. The creation of a standalone residual risk

acceptance component acknowledges that information is not always available, contracts are not always negotiable, and some risks may remain after reasonable mitigation efforts have been exhausted. This suggests the agencies are placing greater weight on how risks are evaluated, governed, and accepted than on whether every potential control or mitigation was pursued. That may be particularly meaningful for bank-fintech partnerships, large service providers with significant negotiating leverage, and longstanding relationships where institutions have accumulated substantial performance history over time.

More flexibility creates potential efficiencies, but also raises the bar for governance

The proposal's emphasis on risk assessment and residual risk acceptance will give banks a practical basis to redirect TPRM resources away from lower-risk relationships and focus more on providers that have more significant potential operational or customer impacts. In particular, the proposal's explicit recognition that community and midsize institutions may require a different TPRM approach than larger organizations provides stronger support for scaled and proportionate oversight practices at these firms.

However, as reinforced by the guidance, banks remain responsible for managing third-party risks that lead to operational disruption, financial loss, legal violations, or customer harm, regardless of how much discretion the guidance provides. In addition, many institutions will still need to identify critical third parties and map dependencies that support important business services to meet the EU's Digital Operational Resilience Act (DORA) and other operational resilience requirements, regardless of the flexibility provided under the proposed guidance.

Banks that amend frameworks to change due diligence standards, negotiate fewer contractual protections, limit inventories, or reduce monitoring activities should support those changes with a well-founded assessment of the likelihood and potential magnitude of harm. While regulators are placing greater reliance on institution-specific judgment, boards and senior management remain responsible for evaluating whether TPRM practices are appropriate for the institution's risk profile. Risk functions and internal audit will need to challenge whether framework changes are appropriate, classifications remain accurate, accepted risks remain within tolerance, and monitoring detects changes before they become material. Documentation will need to connect the risks identified, the oversight selected, the residual risk accepted, and the institution's continuing assessment of the relationship.

What should firms do now? As institutions evaluate the proposal, they should consider:

- **Revisiting risk classification methodologies** to confirm they clearly explain how likelihood and potential magnitude of harm, criticality, concentration, substitutability, operational dependencies, and other factors determine relationship classifications and oversight requirements, while remaining aligned with applicable operational resilience and critical-service mapping requirements.
- **Aligning oversight activities to assessed risk** by evaluating whether due diligence, contracting, monitoring, inventory, and reporting standards are appropriately differentiated across third-party relationships with a focus on those that present the greatest operational, compliance, financial, customer, and concentration risks.
- **Strengthening documentation of residual risk acceptance** by clearly defining decision authorities, documentation expectations, escalation thresholds, and challenge processes for accepting risks that cannot be fully mitigated.
- **Reviewing concentration, dependency, and subcontractor exposures** to ensure that efforts to streamline oversight of lower-risk relationships do not obscure material operational or resilience risks.
- **Enhancing documentation of risk-based decisions** to demonstrate how risk assessments support oversight, resource-allocation, and residual-risk-acceptance decisions and how those decisions align with the institution's risk appetite and tolerances.
- **Revisiting board reporting and governance practices** to ensure directors and senior management have sufficient visibility into relationship classifications, significant residual risk decisions, concentration exposures, and changes in third-party risk, particularly where institutions elect to reduce or streamline oversight activities.

2 CLARITY Act stumbles in Senate as SEC and CFTC vow to move forward

What happened? On September 15th, the Digital Asset Market CLARITY Act [failed to advance](#) in the Senate. The Act received 49 votes to move forward and 50 against, with every Democrat and Independent as well as four Republicans voting not to proceed.

What is in the CLARITY Act? The Act would provide a regulatory framework for digital assets, specifying that the CFTC would oversee “digital commodities” including most non-stablecoin crypto assets such as Bitcoin and Ethereum, while the SEC would oversee “digital securities” such as tokenized securities and assets that constitute investment contracts. It also contains a broad set of requirements around consumer protection, anti-money laundering, restrictions on interest or yield payments, disclosure requirements and bankruptcy protections. For more details, see our previous [Our Take](#) [here](#).

Why did the Act fail to advance? Democrats opposing the bill [called for](#) stronger conflict of interest provisions; stronger anti-money laundering, anti-sanctions and anti-fraud requirements; limitations on “risky” digital asset activity including potential use in retirement funds; and limiting the Act’s preemption of state consumer protection law. Four Republicans voted against the bill as well, with Sens. Josh Hawley (R-MO) and Jerry Moran (R-KS) citing concerns around deposit flight away from community banks.

How did the SEC and CFTC respond? Following the Act’s failure in Congress, SEC Chair [Paul Atkins](#) and CFTC Chair [Mike Selig](#) pledged to continue encouraging digital assets innovation, with Atkins stating that the agency will “act decisively to deliver certainty.” The agencies have since acted on their promises. On September 17th, the SEC [announced](#) a five-year “innovation exemption” that would allow (1) platforms meeting certain criteria to trade tokenized securities without registering as an “exchange” and (2) certain liquidity providers used by tokenized security to avoid being classified as a “dealer” and thereby subject to a broader set of requirements. The following day, the CFTC [submitted](#) to OIRA for review proposals entitled “Regulation Crypto Asset Transactions” and “Regulation Crypto Asset Markets.” The text of these proposals remains non-public while OIRA completes its review.

What’s next? Senators on both sides of the aisle have [pledged](#) to continue negotiating the Act.



Our Take

Agency cooperation continues as CLARITY crumbles

The CLARITY Act is now back to the negotiation table, but the 11-vote gap necessary to pass the Senate combined with a limited remaining legislative calendar and midterm elections around the corner means that it is highly unlikely the bill will make its way to the President’s desk this year. Considering that the Democrats are expected to win a majority of House seats in the next Congress, they will have significantly stronger bargaining power to demand additional protections around areas such as consumer protection, anti-financial crime, preemption of state law and conflict of interest. While many of these areas could reach some form of bipartisan agreement eventually, conflict of interest rules supported by the Democrats would result in a Presidential veto, leaving the Act’s political future one that must be very carefully negotiated if it has any chance of becoming law.

The more immediate future of digital asset market structure regulation now turns to the SEC and CFTC, whose crypto-friendly leaders have pledged to move quickly to provide certainty with or without Congress. Of a laundry list of potential new agency rules and guidance, we expect to see continued joint efforts to develop a taxonomy that would clearly define each agency’s jurisdiction over digital assets (which would largely be in line with the CLARITY Act’s definitions) as well as efforts from the CFTC to create a registration framework for spot exchanges and a framework for leveraged crypto trading.

However, standalone agency action is more prone to legal challenges and less durable than an act of Congress. This is particularly true following recent Supreme Court decisions that (1) provide courts with more power to question agency interpretations and (2) hold that “major questions” (which likely include digital asset regulation) should be answered by Congress instead of agencies’ interpretations of their own abilities. As such, efforts by the SEC and CFTC to provide regulatory certainty likely will receive legal challenges from states and consumer groups, and a future Administration could more easily reverse course on the agency decisions.

3 FDIC Board moves to clear merger pathways and advance deregulatory agenda

What happened? On September 17th, the FDIC held a [meeting](#) at which the Board:

- Issued a [proposal to update its Bank Merger Act \(BMA\) review framework](#);
- Issued a [proposal on state bank parity](#); and
- [Rescinded](#) its 2016 statement on the development and communication of supervisory recommendations.

What would the BMA proposal do? It would substantially revise how the FDIC processes and evaluates merger transactions with a stated goal of improving speed, certainty, and transparency while reducing regulatory burden. Key elements include:

- **Rapid approvals for routine transactions.** The FDIC would create a new category of “de minimis” merger transactions eligible for streamlined letter filings, no public comment period, and deemed approval in as little as five business days for certain qualifying transactions.¹
- **Expanded expedited processing and defined review timelines.** The proposal would establish clearer processing timelines, expand eligibility for expedited review, and require the FDIC to act within specified timeframes depending on the type of transaction.
- **Reduced public notice and comment requirements.** The proposal would reduce publication requirements, shorten the public comment period for certain corporate reorganizations from 30 days to 15 days, eliminate the comment period for de minimis transactions, and limit circumstances in which adverse comments or Community Reinvestment Act protests remove a filing from expedited processing.
- **Modernized competition analysis.** The FDIC would revise its competition framework to incorporate credit union shares and centrally booked deposits into its initial market concentration analysis and establish safe harbors for transactions that remain within specified concentration thresholds.
- **Codified standards for evaluating mergers.** The proposal would place into regulation the FDIC’s approach to evaluating competition, financial and managerial resources, future prospects, community impacts, anti-money laundering controls, and financial stability, replacing reliance on policy statements and providing greater transparency regarding review standards.
- **Greater emphasis on the resulting institution.** The FDIC would place increased weight on the characteristics of the resulting institution and the applicant’s plans to remediate supervisory concerns when evaluating merger applications.

¹ Generally proposed to include (i) merger transactions where the amount of assets acquired by the insured bank would be under the dollar threshold that normally triggers federal antitrust filing requirements for mergers, and the amount of assets acquired would be less than 5% of the acquiring bank’s assets, and (ii) mergers of a bank subsidiary into a bank.

- **New financial stability safe harbor.** The proposal would establish a financial stability safe harbor for certain transactions and a balancing framework for transactions that do not qualify, providing greater certainty regarding how the FDIC evaluates systemic risk considerations.
- **Clearer treatment of mergers in substance.** The proposal would replace the current facts-and-circumstances approach with an asset-based test that generally treats acquisitions of 80% or more of another institution's assets over a rolling 12-month period as a merger in substance. It would also establish a separate notice and non-objection framework for certain significant asset transfers.

What would the state parity proposal do? It clarifies that if a host state's law does not apply to a national bank because federal law preempts that requirement, that law likewise would not apply to an out-of-state bank providing services in that state. Instead, the law of the bank's chartering state would apply. The proposal would not itself determine whether a particular state law is preempted and would not affect state banks' authority to charge interest under Section 27 of the Federal Deposit Insurance Act.

Why did the FDIC rescind the 2016 supervisory recommendations statement? The FDIC rescinded its 2016 Statement on the Development and Communication of Supervisory Recommendations because it has been superseded by the agency's recently finalized framework governing Matters Requiring Attention (MRAs). The 2016 statement provided guidance on the use of supervisory recommendations and Matters Requiring Board Attention (MRBAs), both of which the FDIC has discontinued under the new framework. Going forward, examination findings that require corrective action will be communicated through MRAs

What's next? Comments on the two proposals will be due 60 days after publication in the Federal Register.



Our Take

The FDIC continues to modernize regulation and supervision

The three actions collectively advance the FDIC's broader effort to modernize rules, simplify supervisory processes, and reduce procedural requirements that the agency views as slowing decision-making without materially improving outcomes. In particular, the merger review update proposal is likely to make merger transactions faster and more predictable, with a combination of expedited processing, streamlined procedures, and updated competition analysis. As the FDIC still highlights its consideration of the condition and supervisory record of the resulting institution, firms may benefit from engaging early in the transaction lifecycle, identifying potential concerns before filing, and confirming that remediation progress and strategic objectives are communicated and understood.

Several important elements of the proposal remain subject to comment, including aspects of the revised competition framework and how certain implementation details will operate in practice. Those decisions will ultimately determine the extent to which the proposal changes merger review outcomes, but the overall direction is clear: the FDIC is seeking to make transactions easier to evaluate, faster to process, and more predictable for institutions considering strategic combinations with a potential resulting increase in consolidation and dealmaking.

The state-bank parity proposal and rescission of the 2016 supervisory recommendations statement reinforce the same modernization theme but carry different practical implications. The parity proposal provides some clarity for state-chartered banks operating across state lines without a branch presence (e.g., card-issuing and acquiring banks affected by state interchange or data-usage statutes), but current legal questions related to preemption of state law are unlikely to be resolved quickly. Meanwhile, the rescission of the 2016 supervisory recommendations statement is a procedural step to complete the FDIC's transition to its new MRA framework. Firms should continue aligning with the revised framework, including by updating internal tracking systems, board reporting templates, and remediation governance processes that reference "MRBA" or "supervisory recommendation" terminology.

4 NYDFS details guidance on Part 500 cybersecurity Risk Assessments

What happened? On September 10th, the New York State Department of Financial Services (NYDFS) issued [guidance](#) clarifying expectations for cybersecurity Risk Assessments under Part 500, the New York cybersecurity regulation for its regulated financial institutions, including banks, insurers, mortgage companies, money transmitters, and virtual currency entities.

What does the guidance say? The guidance clarifies existing regulatory requirements and highlights best practices based on weaknesses DFS has identified during examinations and investigations. It is organized around five topics:

1. **Governance and oversight.** Risk assessments should have clear ownership and involve input from relevant business, operations, compliance, legal, IT, and cybersecurity stakeholders. Organizations should communicate material cybersecurity risks identified through the risk assessment process to senior management and, where appropriate, the board or other governing body.
2. **A defined and repeatable methodology.** Organizations should use a consistent approach to identifying, assessing, prioritizing, and documenting cybersecurity risks. The methodology should address relevant threats and vulnerabilities, evaluate likelihood and potential impact, assess the effectiveness of existing controls, distinguish between inherent and residual risk, and be applied consistently so results can be measured and compared over time.
3. **Comprehensive scope and coverage.** Risk assessments should consider the full range of assets and dependencies that could materially affect cybersecurity risk. Beyond requiring an accurate and current asset inventory, DFS highlights a series of considerations for an assessment, including third-party and supply-chain risks, cloud and external service providers, cyber interdependencies, concentration risk, single points of failure, and emerging technologies and threats, including artificial intelligence and advances in quantum computing.
4. **Documentation and traceability.** Organizations should be able to demonstrate how cybersecurity risks were identified and assessed, how those risks are connected to controls or compensating measures, and why risk-acceptance decisions were made. DFS also highlights the value of risk registers or similar mechanisms for tracking remediation, residual risk, and changes over time.
5. **Integration and ongoing updates.** Risk assessments should not be treated as stand-alone compliance exercises. Their results should inform cybersecurity policies, procedures, controls, testing plans, resource allocation, and risk-treatment decisions. Risk assessments must be reviewed at least annually and updated when material business or technology changes alter the organization's cyber risk. Firms should also consider whether changes in the threat environment, critical vulnerabilities, emerging technologies, or geopolitical developments warrant additional updates.



Our Take

DFS highlights need for holistic cybersecurity oversight

Throughout the guidance, DFS positions the risk assessment as the mechanism through which organizations prioritize competing cybersecurity risks and determine where resources and controls are deployed. DFS emphasizes the importance of demonstrating clear, traceable connections from identified risks through control selection, residual risk, risk acceptance, remediation and management decisions. Given DFS's remit across a broad and diverse population of regulated entities, the guidance may also reflect

a widening gap between firms that have operated for years under mature cyber supervisory regimes and those whose risk management practices remain less developed. The release of the guidance suggests DFS continues to encounter weaknesses in how organizations perform, document, maintain, and use those assessments.

Key inputs to understanding a firm's cyber risk profile, such as asset inventories, third-party dependencies, concentration risk, governance structures, testing activities, and risk treatment decisions are often managed through separate processes by different stakeholders. As IT environments become more interdependent, DFS reinforces that bringing those inputs together into a consistent view of cyber risk and resilience that spans technologies, business silos and risk scenarios can become difficult – but is necessary for appropriate risk management. The guidance reflects this reality by highlighting challenges from concentration risk, cyber interdependencies, cloud providers, software supply chains, and emerging technologies. Firms must recognize that in the current environment, risks associated with individual systems, vendors, or business processes can appear manageable in isolation but lead to more significant exposures when viewed collectively across the enterprise.

Insurers provide a useful example. Many carriers operate across legacy platforms, cloud environments, third-party administrators, data providers, outsourced technology services, and expanding AI-enabled capabilities. A single business process, such as underwriting or claims handling, may depend on multiple systems, vendors, and data sources, each owned or managed by different stakeholders. That can make it difficult to maintain a current view of risk, evaluate how changes in one area affect others, and determine where remediation efforts, investments, or additional controls will have the greatest impact.

What should firms do now? NYDFS-supervised organizations should ensure they have the capabilities needed to risk manage their cybersecurity profile and, in particular, consider:

- **Assessing concentrations and dependencies** to identify where cloud providers, technology platforms, service providers, data providers, or other shared resources could create single points of failure or amplify the impact of a cybersecurity event across multiple business functions.
- **Strengthening governance around risk acceptance and remediation decisions** by clearly defining decision authorities, documentation expectations, escalation thresholds, and challenge processes for risks that cannot be fully mitigated or where remediation efforts must be prioritized.
- **Enhancing traceability between identified risks and cybersecurity activities** to demonstrate how risk assessments support control selection, testing plans, remediation priorities, resource allocation, and broader cybersecurity program decisions.
- **Refreshing risk assessment methodologies and supporting inventories** to ensure they remain responsive to evolving technologies, third-party relationships, concentration risks, business operations, and changes in the threat environment.

5 New Cayman AML rule goes into effect

What happened? On September 18th, the Cayman Islands Monetary Authority (CIMA) enacted a [AML compliance program rule](#) alongside a companion [sanctions rule](#) and [FAQs](#). They apply to all financial service providers regulated or licensed by CIMA, including registered investment funds.

What does the rule require? The rule codifies existing guidance rather than creating new expectations entirely. Key highlights include:

- **Risk-based approach.** Firms must document their inherent and residual risk, apply a consistent risk-rating and aggregation methodology, and update mitigation measures without delay when trigger events occur, such as significant changes in business activities, customer populations, products, service providers, jurisdictions, or other developments that materially alter the firm's risk profile.

- **Independent audit.** Firms must conduct risk-based audits, with internal audits capped at two consecutive cycles before the next must be conducted externally. Audits must document auditor independence, and CIMA requires filing of audit reports along with a remediation plan for any deficiencies.
- **Outsourcing.** Firms must conduct due diligence on service providers, assess outsourcing risks, notify CIMA of material outsourced compliance functions, and ensure outsourcing arrangements do not impair regulatory access to information, systems, or records.
- **Governance.** Firms must maintain a documented governance framework, designate an Anti-Money Laundering Compliance Officer with sufficient authority and independence, and ensure the governing body receives appropriate reporting and oversight information.
- **Training and employee screening.** Firms must maintain documented AML training programs, deliver ongoing training appropriate to employee responsibilities, and implement screening procedures designed to ensure personnel are fit and proper for their roles.



Our Take

From guidance to binding obligation, from discrete requirements to broad program expectations

While the rule is framed as a clarification and codification of existing requirements rather than a new AML framework, it gives CIMA a much more detailed basis for evaluating and enforcing how firms govern, implement, and oversee their compliance programs. Historically, many firms have relied on a combination of internal controls, service-provider assurances, group-level frameworks, and periodic reviews to support compliance. The rule places greater emphasis on evidencing how compliance decisions are governed, challenged, and overseen in practice. This may be particularly challenging for investment funds and other entities that rely heavily on administrators, group functions, and third-party service providers. In those models, boards and governing bodies may need to place greater reliance on independent assurance when assessing whether outsourced compliance activities are operating effectively and providing sufficient visibility into emerging risks.

What should firms do now? As firms review and implement the rule, they should consider:

- **Assessing independent audit provider qualifications and availability.** Firms that have used internal resources for two consecutive cycles should evaluate whether alternative providers may be needed to satisfy the rule's external rotation requirement and be aware that demand for qualified independent auditors with Cayman expertise will see significant tightening as a response to the rule.
- **Confirming completeness of audit scope.** The rule's requirement that audits cover the entire compliance program may require firms to look beyond reviews of individual controls or outsourced functions and consider whether they have a comprehensive view of compliance performance across the organization.
- **Reviewing outsourcing agreements for compliance.** Firms should confirm that outsourced and group-level arrangements preserve CIMA's access to data and systems and that they notify CIMA of any arrangement covering a material compliance function. They should also evaluate whether due diligence, monitoring, and governance processes provide sufficient oversight of third-party providers and support the firm's ability to demonstrate compliance with its own obligations.
- **Enhancing risk assessment processes.** Firms should assess whether risk assessment processes are sufficiently integrated into governance and compliance activities and whether they can efficiently incorporate changes resulting from new products, customers, business activities, or other material developments.



On our radar

Fed previews stress testing reforms and expanded supervisory use. On September 18th, Fed Vice Chair for Supervision Michelle Bowman [spoke](#) on upcoming actions to increase transparency of stress-test models and scenario design and reduce volatility in stress-capital-buffer requirements. Separately, she previewed a broader supervisory use of forward-looking scenario analysis and reverse stress testing to identify firm-specific financial and nonfinancial vulnerabilities.

Fed announces initial findings from independent review of Silicon Valley Bank failure. On September 18th, Fed Vice Chair for Supervision Michelle Bowman [announced](#) initial findings from an independent review of SVB's 2023 failure. The review found that supervisors knew or should have known about key vulnerabilities as early as March 2022 but did not take prompt action, citing supervisory risk aversion and unclear decision-making authority as contributing factors.

Agencies issue FAQs on digital identity verification under CIP rule. On September 8th, the OCC, FinCEN, Fed, FDIC and NCUA [issued](#) FAQs addressing state-issued mobile driver's licenses and other verifiable digital credentials under the Customer Identification Program. The agencies stress that the FAQs do not change existing BSA requirements or create new supervisory expectations.

Agencies expand eligibility for extended exam cycle. On September 10th, the OCC, Fed, and FDIC [published](#) an interagency interim final rule amending eligibility requirements for the 18-month on-site examination cycle, pursuant to the 21st Century ROAD to Housing Act.

Agencies issue statement on community bank engagement with core providers. On September 11th, the Fed, OCC, and FDIC [issued](#) a statement clarifying their risk-based supervision of core providers for Community Bank Organizations (CBOs). The statement outlines factors that CBOs should consider when making supervisory allocation decisions regarding these core providers.

Senate Banking Committee advances CFPB nomination. On September 17th, the Senate Banking Committee voted to advance the [nomination](#) of Brian Johnson to serve as CFPB Director.

SEC greenlights Intercontinental Exchange Clear Credit. On September 9th, the SEC [published](#) a notice that broker-dealers may include debit in customer and PAB reserve computations when they post cash, Treasury securities or qualifying customer securities to ICE Clear Credit (ICC) to meet margin requirements.

SEC proposes rescinding shareholder proposal rule. On September 16th, the SEC [proposed](#) a rescission of its shareholder proposal rule while proposing [amendments](#) to give companies more flexibility on discretionary authority and to give shareholders more control on proxy votes.

SEC receives exchange registration filings. On September 11th, the SEC published notices acknowledging that it received Form 1-N filings from [Coinbase Derivatives](#), LLC, [KalshiEX](#) LLC, and [Bitnomial Exchange](#), LLC registering as a national securities exchanges solely for the purposes of trading security futures products.

CSBS published discretionary AI Supervisory Framework. On September 16th, the Conference of State Bank Supervisors (CSBS) [released](#) an AI framework for state examiners to help identify and assess AI utilization at bank and nonbank institutions.

UK and US authorities hold joint tabletop on CCP solution. On September 3rd, senior officials from the CFTC, SEC, FDIC, Fed, and Bank of England [convened](#) for a tabletop exercise on the hypothetical resolution of central counterparties (CCPs). Discussions focused on recent joint work on information sharing and communications arrangements supporting financial stability in a CCP resolution scenario.



Additional information

For additional information on the Our Take series or PwC's Risk and Regulatory Practice please contact:

Amanda Cox

Partner
773 456 5019
amanda.cox@pwc.com

Dietmar Serbee

Partner
917 902 6382
dietmar.d.serbee@pwc.com

Martha Pampel

Managing Director
312 833 3385
martha.pampel@pwc.com

Stein Berre

Managing Director
929 808 7076
stein.berre@pwc.com

Contributing authors: Dean Spitzer, Andrew Namoury, Stephanie Hardt, Matthew Blumenfeld, Andrew Hillyer, David Sherwood, Nate Herrmann, Michael Marchese, Joseph Santone, Alex Yelverton, Vasilios Chrisos, Eric Lorber, Gregory Calpakis, Antoine de Villoutreys, Matthew Gates, Kelli Dawson, Ciara Plunkett, Matt Coughlin, Michael Horn, Tanya Pazhitnykh, Gigi Elliott and Katie Wen.

[pwc.com](https://www.pwc.com)

© 2026 PwC. All rights reserved. PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.