Deloitte.

Federal banking agencies issue a joint statement clarifying risk-management considerations for crypto-asset safekeeping

On July 14, 2025, the Office of the Comptroller of the Currency (OCC), the Federal Reserve Board (FRB), and the Federal Deposit Insurance Corporation (FDIC) issued a joint statement clarifying regulatory expectations for banks and financial institutions engaging in crypto-asset custody activities.[1]

This arrives at a pivotal moment, as the digital asset ecosystem continues to evolve and with regulatory agencies seeking to provide clear guidance for engagement with distributed ledger technology and public blockchain networks. In addition to this joint statement, other digital asset-related regulatory and legislative initiatives—including the Guiding and Establishing National Innovation for US Stablecoins (GENIUS) Act and the proposed Digital Asset Market Clarity Act of 2025—continue to shape the landscape.[2]

The joint statement builds on the March 2025 Interpretive Letter 1183 from the OCC, reaffirming the permissibility of various cryptocurrency activities for national banks and federal savings associations by eliminating previous supervisory requirements, consolidating agency perspectives, and emphasizing effective pro-custody activities and safekeeping.[3] This reflects the new administration's priorities of strengthening American leadership in digital financial technology.

Essential aspects of crypto-asset custody

Custody is increasingly important as financial institutions look to offer a variety of digital asset product offerings, including the ability to engage with stablecoins—a capability that is expected to become a key product offering supporting payments, trading, and other digital asset use cases. Secure and compliant custody solutions will be central to building trust and enabling broader adoption of stablecoins and other digital assets. Cryptographic keys are typically stored in "wallets," which can range from "cold" wallets to "hot" wallets. Proper security requires retaining control over these keys within the wallets and delivering a broad wallet management solution for clients. Custody solutions provide secure storage and management of the private keys associated with stablecoin wallets, enabling the safety of digital assets against theft or loss. By integrating robust custody services, a wallet offering can enhance user trust, facilitate regulatory compliance, and enable seamless transactions for stablecoin holders.

Prior to offering these services, banking organizations must assess key risks such as financial exposures, internal controls, and contingency plans, ensuring board members, officers, and staff have sufficient expertise for safe and compliant operations. Given the rapidly evolving crypto market, firms need flexible risk governance and significant investment in technology and talent to adapt to crypto-asset price volatility—which can affect both service demand and asset values—as well as ongoing technological changes that impact the approach to providing safekeeping services.

Key highlights of the statement

Within the joint statement, the agencies identified six specific areas to ensure effective crypto custody. The practices outlined below are essential for addressing the processes needed to manage digital asset custody solutions effectively and to ensure regulatory compliance, audit readiness, and resilience in an evolving digital asset landscape.

- **General risk management:** Crypto-asset safekeeping requires secure, strong risk management. Organizations that plan to engage in these activities need expertise, adaptable frameworks, and ongoing investment to keep pace with evolving market and technology changes.
- **Cryptographic key management:** Effective crypto-asset safekeeping relies on exclusive control and secure management of cryptographic keys to prevent loss or theft. Institutions should apply strict standards to key management life cycle and sub-custodians, with regular reviews and contingency plans for compromised keys.
- **Audit programs:** Effective risk management calls for audit programs that address all aspects of crypto-asset safekeeping, including third-party risk. Audits should evaluate key management, asset transfer controls, IT systems, and staff expertise, with independent external auditors engaged when internal expertise is limited.
- **Legal and compliance risk:** Those engaging in crypto-asset safekeeping must comply Bank Secrecy Act (BSA)/Anti-money Laundering (AML), Countering the Financing of Terrorism (CFT), Office of Foreign Assets Control (OFAC) , and related regulations, including customer verification and transaction monitoring. Early involvement of compliance leaders and clear agreements to support effective oversight—along with ongoing recordkeeping and transparency—can help manage evolving legal risks.
- **Third-party risk management:** When using sub-custodians or third-party providers for crypto-asset safekeeping, organizations must perform thorough due diligence on controls, key management, and risk practices. They retain responsibility for third-party actions and regulatory compliance and should assess these activities and risks as if their own even when using third-party technology solutions.
- **Additional considerations:** Banks must assess each crypto-asset before safekeeping, as unique key management and integration challenges may arise. Comprehensive analysis should identify technical, operational, legal, and market risks. Ongoing oversight, tailored controls, and independent assurance are essential, along with careful evaluation of the risks associated with different account models, such as omnibus versus separate accounts.

While the joint statement highlights several important risks associated with digital asset custody, there are additional significant risks that banking institutions should recognize and address within their risk management programs.

The joint statement highlights several risk domains that need to be managed to ensure effective crypto custody.

- **Key management risk:** There is a risk of loss, theft, or unauthorized access to crypto-assets due to the compromise of cryptographic keys or sensitive information. Additional risks arise from inadequate, outdated, or poorly maintained cryptographic key management systems. The complexity of managing multiple wallets, key backups, and recovery procedures further amplifies the risk, especially as the number and type of supported assets grow.

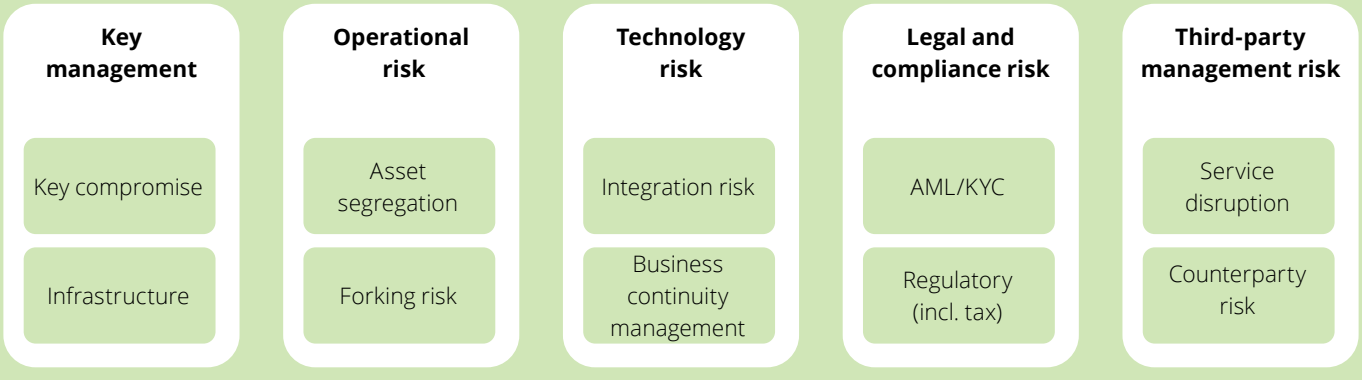
- **Operational risk:** Operational challenges include the management of account structures, such as omnibus versus separate accounts, each of which presents unique risks related to asset segregation, transparency, and client protection. The occurrence of airdrops and forks (i.e., splits) introduces additional complexity by creating new assets or splitting existing ones, which can complicate asset tracking and reconciliation. Frequent changes in asset types, protocols, and settlement methods also heighten the risk of integration failures and operational errors.

- **Technology risk:** Blockchain technology introduces unique technology risks, such as protocol upgrades, the integration of new transaction types or consensus mechanisms, and the need to maintain compatibility with evolving digital asset standards. Insufficient technical expertise can lead to failures in adapting to these changes, increasing the likelihood of system outages, data loss, or security vulnerabilities.

- **Legal and compliance risk:** The evolving regulatory landscape for crypto-assets introduces significant legal and compliance risks. Organizations must comply with a complex web of requirements, including BSA/AML, CFT, OFAC, and state-level regulations, which may be subject to frequent change or inconsistent interpretation. The evolving tax landscape adds further complexity, as tax authorities continue to refine guidance on the classification, reporting, and taxation of digital assets. There is also a risk of customer misunderstanding regarding banks' responsibilities and the legal status of their assets.

- **Third-party and sub-custodian risk:** Reliance on third-party service providers or sub-custodians introduces risks related to insufficient due diligence, inadequate oversight, and potential mismanagement of client assets. Service disruptions, cybersecurity incidents, or insolvency at a provider can delay or prevent access to assets. There is also a risk that third parties may not maintain proper asset segregation or adhere to the same standards of security and compliance as the primary custodian.

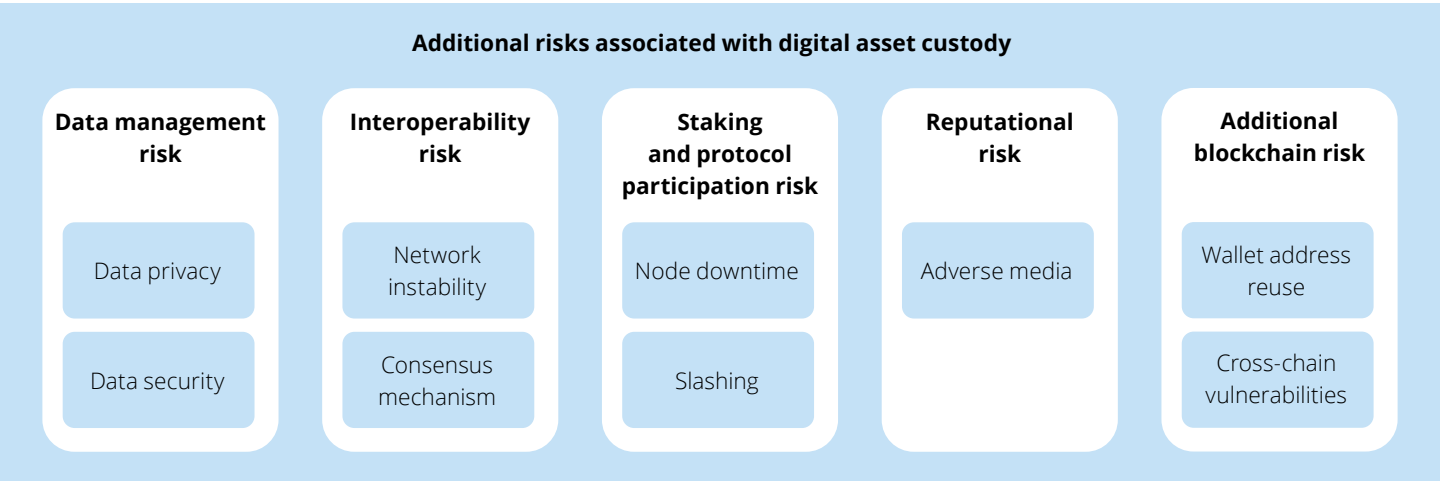
Key digital assets custody risk areas mentioned in the joint statement



In addition to the risks specifically outlined in the joint statement, there are further considerations that institutions will need to proactively manage. They include:

- **Data management risk:** Handling sensitive client and transaction data increases exposure to privacy breaches and regulatory penalties, especially given the complexity of global data protection laws.
- **Interoperability risk:** Reliance on blockchain infrastructure and integration with multiple platforms can lead to node downtime, network instability, or consensus failures and challenges in connecting custody systems with other platforms or blockchains.
- **Staking and protocol participation risk:** Offering staking (blockchain network support) services introduces risks such as slashing (loss of staked assets due to protocol violations), downtime penalties, and smart contract vulnerabilities. Legal and operational ambiguity around the custodian's role in staking, as well as unclear client disclosures, can increase exposure.
- **Reputational risk:** Incidents such as asset loss, service outages, regulatory actions, or negative media coverage can quickly erode client trust and damage an institution's reputation. The high-profile nature of digital assets amplifies the impact of adverse events, making proactive communication and robust incident response essential.
- **Additional blockchain risk:** Additional blockchain-specific risks such as wallet address reuse can compromise privacy, evolving token standards may cause operational disruptions, and cross-chain bridges are susceptible to cyberattacks and asset losses.

Furthermore, the choice between **permissioned and public blockchains** introduces distinct risk considerations. Public blockchains, by design, offer transparency and decentralization but can expose sensitive transaction data to a wide audience, increasing privacy and cybersecurity risks. In contrast, permissioned blockchains provide more controlled access and potentially enhanced privacy, but may introduce risks related to centralization, governance, and reliance on a limited set of validators. Institutions must carefully assess the trade-offs between transparency, privacy, control, and security when selecting the appropriate blockchain architecture for their custody operations.



Broader safety and soundness considerations

As banks deepen their involvement in the digital asset ecosystem—whether through custody, trading, settlement, or other related activities—they are exposed to a **broader spectrum of risks that demand strong risk management**. While regulators have outlined key considerations for crypto custody, they are likely to expect banks to apply **risk and control frameworks that address the full range of operational, compliance, technological, regulatory, and strategic risks associated with digital asset activities**.

Engagement with digital assets goes well beyond safekeeping, exposing banks to evolving challenges as new asset classes emerge. **Risk frameworks need to be continuously updated**, with effective custody beginning by embedding key risk principles into enterprise risk management frameworks, risk appetite statements, and governance structures.

ERM and risk appetite

- Enhance Risk Appetite Statements to cover financial and nonfinancial risks
- Develop a safe and sound risk framework to address operational, technological, capital, and liquidity risks
- Affirm frameworks support expanding digital asset activities

Strategy and product

- Demonstrate product/service has gone through a new approval process
- Conduct ongoing product risk reviews
- Monitor risk relative to the initial product approval

Technology and operations

- Develop technical capabilities to allow the integration with blockchain and digital assets products and services
- Integrate with existing systems to enhance operational resilience
- Actively manage blockchain-specific risks (e.g., protocol changes, smart contract vulnerabilities)

Compliance and regulatory

- Develop compliance programs—including written BSA/AML and OFAC programs—tailored to the bank's products, services, and customer base to include all crypto related activities
- Conduct throughout customer due diligence
- Maintain detailed transactions records
- Report suspicious activities to authorities

Talent capabilities

- Create talent and trainings that are aligned to crypto-banking activities
- Involve risk & compliance experts and product leads & support teams
- Mitigate onboarding risks through specialized expertise

IT reporting and cybersecurity

- Develop a comprehensive IT risk and control framework
- Address IT and information security risks
- Create thorough controls for emerging technology threats
- Establish incident response plans for ransomware, phishing, and vulnerabilities

Key management, security, & storage model

- Establish secure, resilient key management infrastructure, including cold vs. hot storage
- Develop comprehensive key management capabilities (generation, management, destruction, etc.) and robust physical security and access controls, supported by strong backup, recovery, and incident response mechanisms

Third-party risk management

- Establish a safe and sound third-party risk management program that assesses and manages risk posed by third-party relationships (including detailed vendor review process and periodic monitoring of third-party impact)

Tax and accounting

- Establish sound processes for data integrity, asset concentration, and reconciliation
- Manage and address tax implications and accounting challenges to create financial stability and transparency

Audit capabilities

- Audit programs should cover all aspects of crypto-asset safekeeping: key management, asset transfer controls, IT systems, and staff expertise in handling crypto-asset risks
- If internal expertise is lacking, organizations should use independent external auditors to complete a thorough review

Contact us

Leveraging our blockchain-related experience, we have developed a proprietary risk assessment tool composed of more than **300 unique blockchain and digital asset** targeted risks. The tool provides a baseline view of risk applicability across many of the emerging service offerings in the digital asset marketplace, including crypto safekeeping.

Roy Ben-Hur
Managing Director
Deloitte & Touche LLP
rbenhur@deloitte.com

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

Endnotes

1. Federal Deposit Insurance Corporation, Federal Reserve Board, and Office of the Comptroller of the Currency (OCC), "Agencies issue joint statement on risk-management considerations for crypto-asset safekeeping," press release, July 14, 2025.
2. US Congress, S.1582 - GENIUS Act, accessed July 18, 2025; US Congress, Digital Asset Market Clarity Act of 2025 (proposed), July 17, 2025.
3. OCC, "OCC letter addressing certain crypto-asset activities," press release, March 7, 2025.

Deloitte.