PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

Operational Readiness for Tokenized Financial Products

Applying established governance, control and operational discipline to an evolving financial marketplace

By Don Melody, Kevin Keane Jr., Thomas J. DeMayo and Helen Rexwinkel

The conversation around tokenization in financial services has shifted, quietly but meaningfully. For years, tokenization, distributed ledger technology and blockchain-based financial products carried a stigma, particularly among regulated financial institutions and other risk-sensitive market participants. Its association with market volatility, regulatory uncertainty and high-profile failures made many organizations understandably cautious. In some cases, that caution translated into outright avoidance.

Today, that posture is changing. Rather than being viewed primarily as technology associated with speculative markets, blockchain is increasingly being recognized as part of the infrastructure supporting traditional financial markets: a mechanism to improve settlement efficiency, expand access and enable new forms of distribution. If you are interested in this topic, join us for our **Broker-Dealer Symposium** on Wednesday, September 16, at 1:30 p.m. The program will include a panel, *Tokenization of Securities: Is the Capital Markets Revolution Finally Here?*

Large asset managers are exploring tokenized financial products. Platforms are providing blockchain-enabled access to familiar securities. Most importantly, these developments are occurring within or increasingly aligned with established regulatory frameworks.

Perhaps the clearest evidence of this shift is the SEC's evolving approach to tokenization.

- In its December 11, 2025, No-Action Letter, the SEC permitted the Depository Trust & Clearing Corporation (DTCC) to begin exploring tokenization through a controlled pilot program. That program introduces blockchain-based representations of securities positions (or entitlements) while maintaining traditional custody and recordkeeping. This approach reinforces that tokenization is not replacing existing market infrastructure, but rather extending it through the involvement of one of the industry's core market utilities.

- On March 17, 2026, the SEC and CFTC jointly issued long-awaited interpretive guidance clarifying how the federal securities laws apply to certain crypto assets and transactions involving those assets.

Since that guidance, the momentum has continued. Nasdaq has announced implementation plans for 23-hour, five-day-per-week trading. DTCC is expanding clearing capabilities to support extended trading hours and tokenized securities. Institutional asset managers continue to expand offerings backed by real-world assets and broker-dealers are increasingly evaluating stablecoin and blockchain-enabled settlement solutions. Collectively, these developments represent a shift from asking whether tokenization belongs in regulated financial markets to determining how it can be implemented responsibly within them.

Many tokenized financial products are now backed by real-world assets (RWAs), including U.S. Treasury securities, money market funds, equities, private credit and other traditional financial instruments. This evolution is prompting organizations across financial services to evaluate whether their existing operating models, governance structures and reporting processes are prepared for an increasingly digital financial ecosystem.

Tokenized Treasury products, for example, often rely on established asset managers, third-party custodians and frequent, often daily, NAV or pricing transparency. Tokenized equities may, in certain structures, be held with regulated custodians or broker-dealers, even when investor access is provided through blockchain-based platforms.

> "*What makes tokenization particularly significant today is that it is increasingly connecting blockchain technology with financial products and market participants that institutions already understand. The opportunity is no longer just about the technology; it is about integrating that technology into established financial markets in a way that is scalable, controlled and operationally sound.*"
>
> ~ Kevin Keane Jr., Audit & Advisory Partner, PKFOD

These hybrid models help bridge the gap between innovation and trust. They also introduce new operational considerations, including custody, reconciliation, service-provider oversight, financial reporting, tax data flows and cybersecurity, all of which management teams must understand and address.

For broker-dealers, asset managers, investment advisers, fund sponsors, fintech companies and other market participants, the question is no longer simply whether tokenization deserves attention. Increasingly, management teams are asking a more practical question: **Is our organization operationally prepared?** The answer depends less on the technology itself than on the strength of the organization's operating model.

Management teams entering this market are appropriately focused on product development, fundraising, distribution and strategic partnerships. As is often the case with emerging businesses, however, the operational foundation frequently develops later. Governance, custody arrangements, reconciliations, service-provider oversight, financial reporting, tax data flows and cybersecurity controls can quickly become significant business issues as organizations grow or as tokenized activity becomes more material.

The good news is that many of these challenges are not entirely new. While tokenization introduces new technologies, records and counterparties, the underlying governance, operational-risk and control principles remain familiar. At PKF O'Connor Davies, we help financial services clients apply these familiar governance, risk and control principles to new operating models, mapping how accountabilities, controls and service-provider dependencies work across the product lifecycle. Organizations that apply those disciplines early will be better positioned to scale, satisfy regulators and investors and support long-term growth.

1. Who Owns the Operating Model?

A tokenized product can touch product development, operations, finance, compliance, tax, technology, legal and cybersecurity. At PKF O'Connor Davies, our starting point is to work with management to map that end-to-end operating model, so that dependencies and decision points across these functions are visible. Without clear ownership, decisions may otherwise be made within individual functions without sufficient consideration of how the complete operating model supports the organization now and for future long-term growth.

Management should identify who is accountable for the product and who owns the risks created by issuance, trading, settlement, custody, recordkeeping and financial reporting. Roles should be clearly documented, decision rights should be established and significant changes to the product or supporting technology should be subject to appropriate review and approval.

This governance structure should also evolve with the business. A model that is workable during a limited pilot may not be sufficient once transaction volumes increase, additional products are introduced or outside investors and regulated counterparties become involved.

Executive Considerations

- Who has end-to-end accountability for the tokenized product and its supporting operating model?
- Are responsibilities across operations, finance, compliance, tax, technology and cybersecurity clearly defined?
- Who approves material changes to the product, technology or service-provider structure?
- Does the governance model remain appropriate as the business scales?

2. Who Controls the Assets?

Custody and control are fundamental to organizations offering tokenized financial products. Depending on the model, the underlying asset may be held by a regulated custodian, broker-dealer, bank or other third party, while a separate platform records or facilitates transfers of the tokenized interest. Management must understand both the legal custody chain and the practical ability to access, transfer or restrict the related assets.

Authority over wallets, private keys and transaction execution should not depend on one individual. Organizations should establish appropriate segregation of duties, approval requirements, access limitations and contingency procedures. They should also understand how access is granted, monitored and revoked, including when employees or service-provider personnel change roles or leave the organization.

These controls are especially important where a token is represented as fully backed by an underlying asset. Management should be able to maintain clear, reliable evidence of the underlying asset, where it is held, who can move it, how transfers are authorized and how exceptions are investigated.

Executive Considerations

- Where are the underlying assets held, and who has legal custody?
- Who can initiate, approve and execute transfers?
- How are private keys, credentials and wallet access protected?
- Are incompatible responsibilities appropriately segregated?
- What happens if a key employee or service provider becomes unavailable?

PKF O'Connor Davies can help management evaluate custody and transaction workflows, identify control gaps, assess segregation of duties and develop practical procedures over authorization, access and exception management.

3. Can Management Demonstrate That the Records Reconcile?

Tokenized products may rely on several records that were not designed to operate as one system. Our dedicated advisory teams help clients map the flow of information across these records, from blockchain activity and custody records through to administrator and financial-reporting systems. This is particularly important where token activity, underlying assets and investor records sit in different environments.

As tokenized financial products become increasingly integrated into traditional financial markets, management should expect greater scrutiny over the completeness, accuracy and consistency of information flowing between these records.

Differences in timing, data formats, valuation sources and transaction identifiers can make reconciliation difficult. Management should establish a repeatable process that connects token issuance, transfers and redemptions to the underlying assets and to the organization's books and records. Exceptions should be identified promptly, assigned to an owner, investigated and resolved in a documented manner.

A reconciliation process is strongest when it is designed before transaction volumes become significant. Retrofitting controls after a product has scaled can require extensive remediation and can delay financial reporting, regulatory responses, capital raises or strategic transactions.

Management Considerations

Can token issuance and redemption activity be reconciled to the related underlying assets?
Do blockchain, custodian, administrator and internal accounting records agree?
Are timing and valuation differences clearly understood and documented?
Who reviews reconciliation exceptions, and how quickly are they resolved?
Is the process scalable as products and transaction volumes expand?

> *"From an operational due diligence perspective, tokenization does not change the fundamental questions: who controls the assets, how are records reconciled, what happens when an exception arises, and how effectively are critical service providers overseen? The technology may be new, but investors will still expect a resilient operating model and clear evidence that it works in practice."*
>
> ~ Helen Rexwinkel, Head of Operational Due Diligence, PKFOD

4. How Well Does the Organization Know Its Critical Service Providers?

Many tokenized operating models depend heavily on third parties. In our operational-risk and due-diligence work, PKF O'Connor Davies focuses on whether the organization has identified its critical providers, understood the risks they introduce and established proportionate oversight. Custodians, fund administrators, technology developers, wallet providers, cloud platforms and pricing services may all perform activities that are essential to the product; outsourcing those activities does not outsource management's responsibility for the associated risks.

Organizations should perform due diligence before engaging a critical provider and should maintain ongoing oversight after the relationship begins. The review should consider financial condition, experience, regulatory status, cybersecurity, business continuity, incident history, subcontractors and the provider's ability to meet the organization's reporting and control requirements.

Service organization control reports and other independent assessments may provide useful information, but they should be evaluated in the context of the specific services being used. Management should understand the report period, scope, identified exceptions and any complementary controls that the organization itself must operate.

Management Considerations

- Which third parties are critical to the product and its day-to-day operation?
- What due diligence was performed before each provider was selected?
- How are performance, cybersecurity and control issues monitored over time?
- Are relevant SOC reports or other independent assessments available and reviewed?
- What contingency plans exist if a critical provider fails or experiences a prolonged outage?

5. Can Financial Reporting, Accounting and Tax Data Flows Keep Pace?

An organization may successfully launch a tokenized financial product while still facing significant accounting and tax challenges. Tokenized business models can generate new transaction types, revenue streams, entity relationships and cross-border data flows. The accounting system must capture the activity completely and accurately and the information needed for tax reporting must be available in a usable form.

Management should consider how token activity enters the general ledger, how revenue and fees are recorded, how assets and obligations are classified and how valuations are supported. The organization should also identify the data required for federal, state, local and international tax compliance, including transaction-level information that may not be readily available from the operating platform.

Addressing these questions early can reduce the risk of manual workarounds, inconsistent reporting, costly system changes and unexpected tax consequences. A coordinated approach is particularly important because the accounting treatment, legal structure, regulatory classification and tax analysis may influence one another.

At PKF O'Connor Davies, our deep bench of specialists across these functions focuses on working together with clients to consider these issues as a single workstream, ensuring we solve them for the complete picture. Examples of our support include process design, accounting-system integration, financial-reporting assistance, tax data planning and coordination across the organization's internal and external specialists.

Management Considerations

- Does the accounting system capture all relevant token activity and related fees?
- Are revenue, asset classifications and valuation methods documented and consistently applied?
- Can management produce reliable financial information on a timely basis?
- Is transaction-level information available for tax reporting and compliance?
- Have accounting, legal, regulatory and tax considerations been evaluated together?

6. Is the Cybersecurity and Incident-Response Program Ready?

Tokenized products can create concentrated cybersecurity risks because access credentials, wallets, smart-contract functionality and interconnected service providers may directly affect the ability to control or transfer assets. A single compromised credential or signing key can move assets in minutes and unlike a traditional wire transfer, an on-chain transfer generally cannot be recalled. Where the product runs on a public chain, the environment is also public and permanent. Wallet addresses, transaction histories, contract code and balances are visible to anyone and attackers use that visibility to pick targets and time their moves. Anything written to the chain cannot be erased, so personal data and investor identifiers should never touch it. The chain should carry references. Sensitive data belongs in systems the organization controls.

Key management is the control that matters most. A signing key is the asset. Anyone who holds it can move funds, whether that is an insider acting alone or an external attacker who phished a credential or compromised an administrator's endpoint. Controls should assume both. Keys should be protected with hardware security modules or multi-party computation and no material transfer should execute without quorum approval. Quorum only works if each approver verifies the transaction on the signing device itself.

The largest thefts in this market did not break the cryptography. Attackers fed approvers a screen that did not match the payload. Hot wallets should hold only what daily operations require, with the balance in cold storage. The strategy should also weigh whether the organization should hold keys at all. Qualified custodians can take on key custody under a regulated framework and for many organizations that is the more defensible answer. Wherever keys reside, recovery procedures should be documented and rehearsed, not assumed.

> "*The wallet doesn't hold the asset. It holds the key the asset trusts, and the asset can't tell the difference between you and a thief.*"
>
> ~ Tom DeMayo, Partner, Cybersecurity and Privacy Advisory, PKFOD

Smart contracts demand the same rigor. Code should receive independent security review before deployment. Administrative functions such as minting, pausing and upgrades should require multi-party approval, with timelocks where appropriate. Where the product relies on oracles or bridges, those dependencies should be inventoried and monitored. Monitoring should also extend on-chain. Transfers outside approved patterns and unexpected contract interactions should generate alerts that a named individual owns.

Incident-response plans should identify who makes decisions and how fast the organization can act. That means pausing a contract, moving assets off a compromised key, suspending transfers and getting the custodian on the phone. The window to act on a stolen key is measured in minutes, not days. Notification obligations to regulators and counterparties should be mapped in advance and evidence preserved across both on-chain records and off-chain logs. Plans should be tested against scenarios such as a stolen signing key or a malicious contract upgrade and updated as the product, technology and vendor structure change.

Management Considerations

- Who holds signing authority over wallets, platforms and critical infrastructure, and can any individual act alone?
- Should the organization hold its own keys, or does a qualified custodian reduce the risk?
- Can approvers verify what they are actually signing?
- Are changes to code, smart contracts and system configurations independently reviewed?
- Can suspicious on-chain activity and operational exceptions be detected and acted on promptly?
- Has the incident-response plan been tested against tokenization-specific scenarios?

7. Bringing the Disciplines Together

As tokenized financial products become more closely integrated into traditional financial markets, organizations often discover that the most significant challenges are not limited to the technology itself. They arise at the points where the technology connects to people, processes, service providers, financial records, tax reporting and regulatory responsibilities.

The organizations best positioned for sustainable growth will be those that combine innovation with clear governance, effective custody and access controls, reliable reconciliations, disciplined third-party oversight, scalable financial reporting and tax data flows as well as cybersecurity designed for an environment that is public, permanent and unforgiving. These are established business disciplines, but they must be deliberately adapted to the specific tokenized structure.

> *"As tokenized financial products move further into regulated markets, the technology will continue to evolve, but the fundamentals will not. Strong governance, reliable financial reporting and effective controls will remain essential to earning the confidence of regulators, investors and other market participants."*
>
> ~ Don Melody, Audit & Advisory Partner, PKFOD

Contact Us

PKF O'Connor Davies helps financial services organizations apply these established disciplines through our Financial Services Advisory, Operational Risk, Cybersecurity, Tax, Fund Administration and Outsourced Accounting professionals. By helping clients address operational readiness early, we enable management teams to focus on developing innovative products while building the governance, controls and infrastructure needed to support sustainable growth, regulatory expectations and stakeholder confidence.

If you have any questions, please contact your client service team or:

Don Melody, CPA, CFE
Partner
dmelody@pkfod.com |646.893.0178

Kevin Keane Jr., CPA
Partner
kkeanejr@pkfod.com | 646.600.2881

Thomas J. DeMayo, CISSP, CISA, CRISC, CEH, CHFI, CCFE, CMMC-CCA
Partner
tdemayo@pkfod.com | 646.449.6353

Helen Rexwinkel, CA
Partner
hrexwinkel@pkfod.com | 203.323.2400

This article was originally published on August 26, 2026.