KPMG Point of View On Internal Audit & Controls

Digital assets in banking

Internal Audit for the On-Chain Era



kpmg.com

2026

Contents

Executive summary 2

Regulatory update 3

Use cases & Internal Audit priorities 4

Digital asset payments 5

Cross-Cutting disciplines & OCC risk taxonomy 8

Vendor governance—TPRM deep dive 10

The blueprint & next steps 11

How KPMG can help 12

© 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS043975-2A

Executive summary

The window to prepare is closing.

Digital assets are transitioning from niche technology applications into the core of institutional banking. Stablecoins, tokenized deposits, tokenization, on-chain payments, and custody are rewiring transactional infrastructure—and with it, the operational, compliance, and risk profile of the institution.

While regulatory guidance continues to evolve, one principle that remains clear is that banks retain ultimate accountability for operational resilience and compliance—regardless of third-party outsourcing, vendor models, or participation in industry consortiums.

Recent milestones have begun to shape the US framework. The Guiding and Establishing National Innovation for US Stablecoins Act (GENIUS Act) established the first legislative framework for stablecoins, focusing on key areas such as licensing, reserve requirements, and enterprise risk management. The Securities and Exchange Commission (SEC) has rescinded Staff Accounting Bulletin (SAB) 121 in favor of a principles-based SAB 122, removing major barriers to bank-offered custody for digital assets. The Office of the Comptroller of the Currency (OCC)'s Interpretive Letter 1183 reaffirms permissible banking involvement while removing the "supervisory non-objection" safety net.

> "Digital assets don't replace the risks banks already know—they change where those risks sit and how they show up. The challenge for Internal Audit is understanding where blockchain, smart contracts, wallets, and custody break the assumptions our traditional control frameworks were built around. That's where the audit approach has to evolve."



Paul Heidler
Managing Director
Internal Audit & Controls Digital Asset Leader
KPMG LLP

© 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS043975-2A

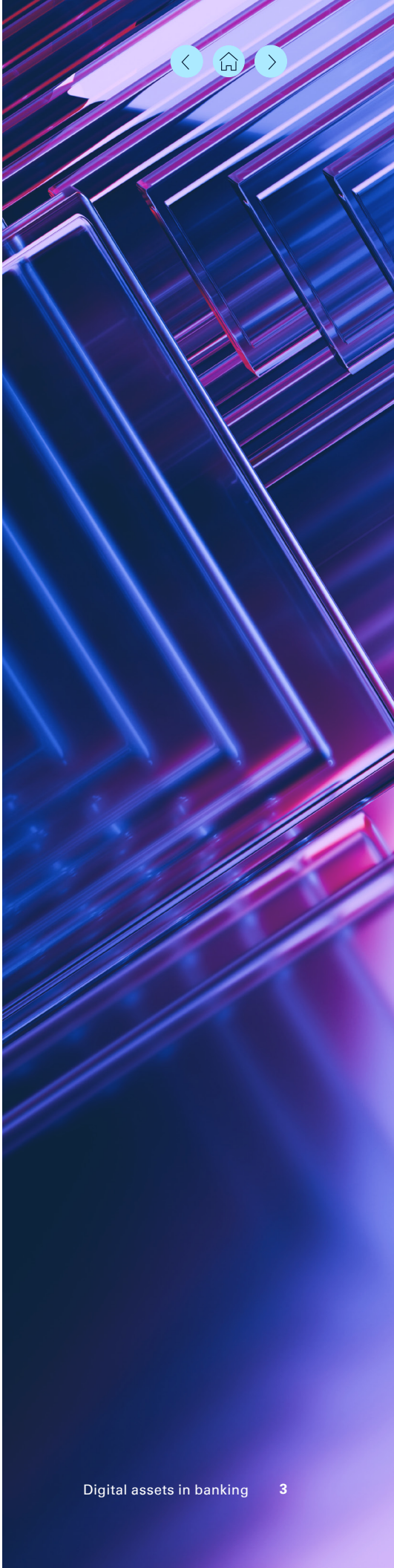
Regulatory update

From enforcement-led to compliance-first.

The US landscape is transitioning to a structured, compliance-first framework. For Internal Audit, these milestones change both what must be audited and how audit risk is evaluated for digital asset products and services.

Recent regulatory developments have reduced longstanding barriers and provided greater clarity around banks' participation in digital asset products and services. Collectively, the milestones listed below are helping shift the industry from regulatory uncertainty toward a more defined framework for custody, stablecoin issuance, and other digital asset products and services. Additionally, these events have laid the foundation for banks and other financial institutions to revisit their digital asset strategies in a regulatory compliant way.

Milestone	Operational & Financial impact
SEC SAB 122 JAN 2025	Removes the on-balance-sheet liability for safeguarded digital assets, unlocking scalable, bank-grade digital custody offerings.
OCC Interpretive Letter 1183 MAR 2025	Reaffirms that custody, stablecoin, and distributed-ledger activities are permissible for national chartered banks—without prior supervisory non-objection.
FDIC FIL-7-2025 MAR 2025	Rescinds prior notification requirement for FDIC-supervised institutions, allowing banks to engage in permissible digital asset activities without prior FDIC approval.
Federal Reserve APR 2025	Rescinded previous supervisory letters from 2022 and 2023 that required state members provide advance notification of planned or current crypto-asset activities, and required a nonobjection process for state member banks to engage in dollar token activities, respectively.
GENIUS Act JUL 2025	Establishes the first legislative framework for stablecoins, with requirements for licensing, reserves, capital, risk management, custody, etc.
SEC/CFTC "Project Crypto" MARCH 2026	Unified rulebook and stable "token taxonomy" clarifies federal securities laws for digital assets, moving from ad-hoc enforcement to a compliance-first regime.



© 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS043975-2A

Where to focus, and why.

An effective audit strategy starts with categorizing and prioritizing digital asset use cases by risk profile, their impact across the bank, and impact to the Internal Audit department (increased audit coverage, supplemental subject matter expertise, etc.).

The following table assesses common digital asset use cases based on their risk profile and resulting impact on Internal Audit coverage, auditor skillsets, and audit complexity.

Use case	Business Context	Primary Risk Drivers	Specialized Skillset	Audit Complexity
Stablecoin Issuance	Broad applicability under the GENIUS Act	Operational Compliance Financial	HIGH	HIGH
Payments & Settlement	Alters transaction flow, transaction costs, speed of settlement, and payment rails via stablecoins that transact on public blockchains.	Operational Compliance Financial	HIGH	HIGH
Tokenized Deposits & Interbank Clearing	Bank-led networks (e.g., The Clearing House—25+ banks) for programmable, 24/7 movement linking on-chain and fiat rails.	Strategic Operational Financial	MODERATE	HIGH
Custody	Foundational infrastructure for private key management used to secure digital assets using institutional grade custody platforms—accelerated by SAB 122.	Operational Cyber/Tech Financial	VERY HIGH	VERY HIGH
Trading & Brokerage	Multi-asset execution and liquidity sourcing across external liquidity providers (LP) and exchanges that enable customers to buy, sell, and hold digital assets.	Compliance Financial	HIGH	HIGH
Tokenization of Real-World Assets (RWAs)	Structuring and deploying traditional securities such as money market funds (MMFs), stocks, and bonds onto blockchains on-chain liabilities and securities	Strategic Compliance	HIGH	MODERATE

The regulatory update and milestones outlined above have helped create the conditions for banks to pursue a broader range of digital asset products and services. However, the resulting impact to Internal Audit is driven by the specific use cases adopted and their associated risk profiles. Internal Audit should assess how each use case will change the organization's risk universe, audit coverage, specialized skillsets, and overall audit complexity. Internal Audit priorities should be aligned to the nature, scale, and maturity of the bank's digital asset footprint.

© 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS043975-2A

Digital asset payments

The end-to-end digital asset payment lifecycle.

Digital asset payments are proving to be one of most widely adopted use cases at banks given their speed of settlement, lower cost of transactions, and 24x7 operations. This step-by-step lifecycle breakdown provides illustrative activities with an OCC risk stripe lens, highlighting the potential areas Internal Audit should focus.

1. Customer Onboarding
2. Fiat → Digital Assets
3. Payment Initiation
4. Pre-verification
5. On-Chain Execution
6. Post Settlement & Reconciliation
7. Digital Assets → Fiat

© 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS043975-2A

Stage	Activities	OCC Risk stripes	Internal Audit Focus
01 Customer Onboarding	**Identity—Know Your Customer (KYC)—Disclosures** • KYC identity verification • Source-of-funds review on fiat • Authorized wallet creation • Disclosures & terms acceptance • Risk rating & ongoing due diligence	Compliance (Financial Crimes) Operational	Validate KYC and source-of-funds policies. Transaction monitoring and sanction screening. Verify adequacy and communication of customer risk disclosures.
02 Fiat → Digital Asset	**Liquidity—Conversion** • LP • Counterparty risk management • Price risk & spread monitoring • Conversion limits & thresholds • Withdrawal process • Client request & fund verification	Financial (Liquidity, Credit, Price) Operational Compliance	Audit LP onboarding, counterparty exposure limits, pricing spreads, and client fund sufficiency prior to executing conversions. Assess relevant third-party controls and SOC coverage where applicable.
03 Payment Initiation	**Authorization—Limits** • Reg E disclosures • Verification of funds • Limit thresholds & velocity • Fee & FX rate confirmation	Financial (Price) Operational Compliance	Evaluate Reg E compliance. Validate automated fund-verification routines and limit/velocity throttling controls designed to mitigate errors and fraud.
04 Screening & Whitelisting	**Screening—Whitelisting** • Wallet whitelisting (Travel Rule) • OFAC sanctions screening • Address verification • Net payment pricing disclosure	Compliance (Financial Crimes) Financial (Price) Operational	Verify OFAC screening operates pre-execution. Address verification, Travel Rule implementation, use of whitelisting, and pricing disclosures.
05 On-Chain Execution	**Settlement Signing** • Hardware Security Modules (HSM)/ Multi-Party Computation (MPC)/ Multi-sig signing • Blockchain transaction construction • Gas/network fee management • API & key security controls	Operational Financial (Price)	Review private key management procedures including use of HSMs/ MPC, key generation processes, segregation of duties, and transaction authorization limits. Assess key backup/recovery and operational resiliency controls. Review API connections and transaction construction. Validate accounting treatment for gas/network fees.

© 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS043975-2A

Stage	Activities	OCC Risk stripes	Internal Audit Focus
06 Post Settlement & Reconciliation	**Reconciliation & AML** • On-chain ←→ omnibus reconciliation • Settlement break investigation • Reserve verification (if needed) • AML transaction monitoring • On-chain analytics & Suspicious activity reports (SAR) escalation	Operational Financial (Liquidity, Credit) Compliance	Test the real-time reconciliation between internal ledgers and blockchain data. Audit break investigation workflows, AML monitoring, and SAR escalation. Liquidity and capital reserve maintenance.
07 Digital Asset → Fiat	**Exit Payout Reporting** • LP • Limit & conversion timing • Price risk at conversion • Client verification & payout rails • Information reporting (1099/CTR) • Accounting—principal vs. agency	Financial Operational Compliance Strategic	Test conversion pricing, timing, and liquidity reserves. Validate payout rails and customer verification. Audit 1099/CTR reporting and principal-vs-agency accounting treatment.

Examples of why on-chain activity creates new and/or additional risks

Risk Consideration(s)	The Description
Irreversibility & Settlement Finality	Blockchain transactions are irreversible and cannot be recalled like traditional payment transactions, increasing the importance of preventive controls.
Wallet/key risk	Digital assets are bearer instruments and anyone with knowledge of the private key for a particular address can transact with those funds. As a result, compromise, loss, or theft of private keys can lead to permanent loss of funds.
24/7/365	Blockchain networks operate 24 hours a day, 7 days a week, creating different expectations for monitoring, incident response, reconciliation and liquidity management.
Financial Crimes	Sanctions/AML controls should incorporate wallet addresses, blockchain analytics, transaction tracing and travel rule considerations alongside robust KYC procedures.
Third-Party & Technology Dependencies	Exchanges, custodians, LP, smart contracts, and blockchain networks can introduce risks outside the bank's current environment. Outsourcing these critical functions will not absolve the bank from the risks that they present.
Internal Skillsets	Banks have historically not offered digital asset products and services. As such, many stakeholder groups across the organization are not well-equipped to manage the unique blockchain risks that accompany digital asset offerings that banks are moving forward with.

© 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS043975-2A

Cross-Cutting disciplines & OCC Risk taxonomy

Applied horizontally. Across every stage.

Digital asset activities do not exist in isolation. Internal Audit should validate that critical program-level disciplines apply horizontally across all seven lifecycle stages.

Risks & Considerations	Strategic Internal Audit focus
Disaster Recovery & Resiliency	Validate Recovery Time Objective (RTO)/Recovery Point Objective (RPO) for on-chain and off-chain components; test failover for signing infrastructure and node connectivity.
Cybersecurity & Key Management	Independently challenge HSM/MPC architecture, key-ceremony evidence, and access-recertification cadence.
Data Governance & Lineage	Verify on-chain/off-chain data reconciliation, immutability assertions, and audit-evidence retention for regulator inquiries.
Model Risk & Pricing	Validate stablecoin reserve attestations, conversion-pricing models, and slippage assumptions under stress.



© 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS043975-2A

OCC Risk Taxonomy—Mapped to Digital Asset Vulnerabilities

Stage	Sub-Categories	Vulnerabilities	Internal Audit Challenge & Response
01 Financial	Liquidity Credit Price Interest Rate	Settlement mismatches between near-instant chains and slower fiat rails; price spreads during conversion; LP counterparty exposure.	Audit intraday liquidity stress-testing, evaluate counterparty credit limits, validate automated price/FX-spread monitoring.
02 Operational	Cyber Security Third-Party	HSM/MPC vulnerabilities; API/ node failures; key custody and wallet/address input errors; third-party and infrastructure concentration; blockchain network disruption or protocol changes, inadequate due diligence over supported assets and service providers.	Assess cryptographic key management, evaluate third-party due diligence, concentration risk and exit planning; assess governance over blockchain/network and supported-asset selection; test continuity and recover across digital asset infrastructure.
03 Compliance	Financial Crimes (FINC) · Regulatory	High-velocity financial crimes; failure to apply Travel Rule whitelisting; inadequate non-FDIC disclosures; delayed batch sanctions screening; inadequate coin-listing criteria	Validate pre-execution sanctions screening. Integrate blockchain-native analytics tools for SAR escalation.
04 Strategic	N/A	Poor alignment with bank-led clearing networks; agency vs. principal model missteps; displacement by tokenized bank-led liabilities.	Review the digital asset roadmap, assess consortia alignment, and challenge the Board-approved risk appetite.

© 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS043975-2A

Vendor governance—TPRM deep dive

Reliance is not a transfer of accountability.

Banks increasingly rely on specialized digital asset service providers for custody, wallet operations, settlement, tokenization infrastructure, blockchain analytics, and compliance workflows. While many providers operate under their own regulatory framework, banks remain accountable for outsourced activities and must determine whether vendor controls, reporting transparency, staffing models, and testing rigor are aligned to the heightened expectations applied to large, highly regulated banking organizations.



Watch-Out

Outsourcing does not transfer accountability for managing risk. Banks remain accountable for digital asset activities performed by third-parties and should assess whether third-party providers maintain appropriate controls over key risks, including but not limited to: private key management, transaction monitoring, sanctions screening, blockchain and coin selection assessments, etc. Internal Audit should evaluate both the effectiveness of third-party oversight and the underlying control environment rather than relying solely on contractual protections or third-party assurance reports.

© 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS043975-2A

A four-step modernization framework.

To evaluate digital asset operations, Internal Audit should update its audit universe, risk assessment, control testing approach, and coverage priorities. Each step below is paired with a diagnostic question every Chief Audit Executive (CAE) should be able to answer.

1 Determine How Digital Assets Impact the Audit Universe

Map digital asset activities across products, legal entities, technology platforms, third parties, and shared networks—including custody, tokenized deposits, stablecoins, wallet operations, settlement, and blockchain analytics.

Question: Have digital asset risks (smart contracts, private key compromise, accounting treatment, third-party dependencies) been integrated into the enterprise risk taxonomy and the audit universe?

2 Perform Targeted Risk Assessments

Conduct risk assessments at the use-case and lifecycle-stage level, mapping inherent risks to OCC risk stripes and overlaying vendor and on-chain dependencies.

Question: Are targeted risk assessments performed across digital asset products and business activities, including third-party dependencies such as blockchain analytics tools to identify and assess the likelihood and impact of key inherent risks and inform audit coverage?

3 Refresh Control Testing & Capability

Upskill the audit team on blockchain forensics techniques, private key management, and new or emerging legislative frameworks. Adopt blockchain-native analytics into the testing toolkit.

Question: Does the internal audit team have the technical fluency—or co-sourced specialist access—to independently challenge private key management practices, blockchain transaction monitoring, use of smart contracts, and on-chain reconciliation, rather than relying on first- and second-line attestations?

4 Deploy a Prioritized Coverage Strategy

Sequence multi-year coverage against the institutions planned or implemented use cases (Payments & Settlement, Tokenized Deposits, Custody) and embed continuous monitoring where on-chain transactions allow.

Question: Does our governance provide the Board with timely, decision-useful visibility into operational, liquidity, and regulatory risks from collaborative blockchain network integrations, with defined risk appetite and escalation pathways?

© 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS043975-2A

How KPMG can help

A trusted advisor for the Chief Audit Executive.

The pace of digital-asset adoption is outpacing most Internal Audit functions' ability to hire, train, and execute. KPMG LLP combines deep banking knowledge with digital-asset specialists to help CAEs close capability gaps quickly and credibly.

Ways we engage

Co-Source & Loan-Staff Support

Embed KPMG digital-asset auditors alongside your team on a per-audit, per-quarter, or program basis. Flexible ramp-up preserves your reporting lines while adding blockchain, custody, and stablecoin expertise on demand.

Audit Scoping & Plan Design

Help establish/advise on a right-sized multi-year audit plan—including key controls, testing procedures, and hour budgets—mapped to regulatory expectations.

Full Outsource of Digital-Asset Audits

For institutions without in-house experience, KPMG can execute the full digital-asset audit plan: planning, fieldwork, reporting, and remediation validation—under your Internal Audit methodology and Audit Committee governance.

Vendor, Custodian & Consortia Audits

SOC-style and control-focused reviews of custodians, wallet providers, on-chain analytics vendors, and shared clearing/settlement nodes. Independent validation where SOC 1/2 coverage is thin or absent.

Subject-Matter Professionals on Call

Rapid access to, digital asset custody specialists, on-chain analytics practitioners, digital asset accountants, and former FRB/OCC/SEC regulators to advise on discrete technical issues without a full engagement.

Regulatory Readiness & Exam Support

Prepare for OCC, FRB, FDIC, and state exams covering GENIUS Act, remediation roadmaps, and MRA/MRIA response support, etc.

Enterprise & Audit Risk Assessment

Refresh the Internal Audit risk universe to reflect stablecoins, tokenized deposits, custody, and shared-ledger settlement, etc.

© 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS043975-2A

Start the conversation

Whether you need a single subject-matter professional for a two-week scoping review or a multi-year co-source arrangement covering your full digital-asset audit universe, KPMG can meet you where you are. Contact the KPMG Digital Assets Team.

Connect with our Digital Assets team



Paul Heidler
Managing Director
Internal Audit & Controls Digital Asset Leader
T: 540-219-5809
E: pheidler@kpmg.com



Brian Consolvo
Principal
Advisory Digital Assets Leader
T: 757-646-6378
E: bconsolvo@kpmg.com

Cross-functional Digital Asset contacts

Robert Sledge
Partner
Audit Digital Asset Leader
E: rsledge@kpmg.com

Jamison Sites
Principal
Tax Digital Asset Leader
E: jamisonsites@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: **kpmg.com**

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization. USCS043975-2A