KEVIN D. ODEN & ASSOCIATES LLC

Model Risk Management | Quantitative Analytics | Regulatory Advisory

Stablecoins, the GENIUS Act, and Model Risk:

A Framework for Financial Institutions Navigating the New Regulatory Landscape

Prepared by: Kevin D. Oden, PhD
Founder & Principal, Kevin D. Oden & Associates LLC

February 2026

www.kdoa.com

Executive Summary

The enactment of the Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS Act) on July 18, 2025, followed by the Office of the Comptroller of the Currency's (OCC) subsequent proposed rulemaking, marks a pivotal moment for financial institutions engaging with payment stablecoins. For the first time, federal law defines who may issue a stablecoin, how it must be backed, and which regulator must oversee it. The Act replaces a patchwork of state and federal guidance with enforceable standards for reserve assets, redemption rights, disclosures, custody, and capital requirements, while clarifying that compliant payment stablecoins are neither securities nor commodities.

This white paper provides financial institution executives, risk managers, and boards of directors with a comprehensive understanding of four critical areas: (1) what payment stablecoins are and how they function; (2) the specific risk exposures that stablecoin activities create for financial institutions; (3) how model risk pervades stablecoin operations under the new regulatory framework; and (4) a practical, actionable framework for managing that model risk effectively.

The OCC's proposed rule (12 CFR Part 15, Docket ID OCC-2025-0372) creates model risk obligations across eight dimensions—reserve valuation, liquidity stress testing, interest rate risk, capital adequacy, concentration risk, operational risk, smart contract validation, and monetization capability assessment—each requiring the development, independent validation, and ongoing monitoring of quantitative models and algorithmic systems. Institutions that build robust model risk management frameworks from inception will be best positioned to operate safely and competitively in this new regulatory environment.

1. What Are Stablecoins?

1.1 Definition and Mechanics

A stablecoin is a digital asset—a digital representation of value recorded on a cryptographically secured distributed ledger (such as a blockchain)— designed to maintain a stable value relative to a reference asset, most commonly the U.S. dollar. Unlike volatile cryptocurrencies such as Bitcoin or Ethereum, stablecoins aim to hold a fixed exchange rate, typically 1:1 with a fiat currency.

The GENIUS Act defines a "payment stablecoin" as a digital asset that (i) is designed to be used as a means of payment or settlement, and (ii) whose issuer is obligated to convert, redeem, or repurchase it for a fixed amount of monetary value while representing that it will maintain a stable value. The Act explicitly excludes national currencies, bank deposits (including tokenized deposits recorded on distributed ledger technology), and securities from this definition. This distinction is critically important: tokenized deposits remain bank deposits, entitled to FDIC insurance and subject to existing banking regulations, whereas payment stablecoins are a separate product class under a new regulatory framework.

1.2 How Stablecoins Work

The fundamental operating model of a payment stablecoin involves three core functions:

Issuance (Minting): A user delivers fiat currency or equivalent value to the issuer, which then creates ("mints") new stablecoin tokens on a distributed ledger. The issuer simultaneously acquires reserve assets backing each outstanding stablecoin on at least a 1:1 basis. Smart contracts—self-executing programs deployed on blockchain networks—typically automate the minting process, enforcing rules around supply management and compliance controls.

Circulation: Once minted, stablecoins circulate on public or permissioned blockchains, enabling peer-to-peer transfers without intermediaries, trading on digital asset exchanges, settlement of commercial transactions, and cross-border payments. Transfers occur 24 hours a day, 7 days a week, 365 days a year, settling in seconds or minutes rather than the hours or days typical of traditional payment systems. Some issuers maintain the capability to freeze funds or block transactions involving their stablecoin to comply with legal obligations such as court orders or sanctions enforcement.

Redemption: A stablecoin holder returns tokens to the issuer in exchange for fiat currency at par value. The issuer destroys ("burns") the redeemed tokens, reducing the outstanding supply and correspondingly reducing the required reserve assets. Under the GENIUS Act, issuers are legally obligated to honor redemption requests, creating a binding put option at par value for all stablecoin holders.

1.3 Types of Stablecoin Backing Mechanisms

While the GENIUS Act focuses exclusively on fiat-collateralized stablecoins backed by reserve assets, understanding the broader landscape provides important context for risk assessment:

Fiat-Collateralized (Regulated Under GENIUS Act): These stablecoins are backed 1:1 by cash, bank deposits, Treasury securities, money market funds, repurchase agreements, or other high-quality liquid assets. The reserve assets are held by the issuer or an eligible financial institution custodian. Examples include USDC and USDT (to the extent they comply with the Act's requirements). This is the only category regulated as a "payment stablecoin" under the GENIUS Act.

Crypto-Collateralized (Not Regulated as Payment Stablecoins): These stablecoins are backed by other digital assets, typically overcollateralized due to the volatility of the collateral. The MakerDAO system backing DAI is the most prominent example. Because the backing assets are digital assets rather than the fiat-equivalent reserves required by the GENIUS Act, these do not qualify as payment stablecoins.

Algorithmic (Not Regulated as Payment Stablecoins): These stablecoins use algorithmic supply-and-demand mechanisms (expanding and contracting token supply) to maintain their peg without full reserve backing. The collapse of TerraUSD (UST) in May 2022, which erased approximately $40 billion in market value in a matter of days, illustrated the catastrophic failure mode of this approach. The GENIUS Act does not authorize algorithmic stablecoins as payment stablecoins.

1.4 Permissible Reserve Assets Under the GENIUS Act

Section 4(a)(1)(A) of the GENIUS Act specifies eight categories of assets that permitted payment stablecoin issuers may hold as reserves. The OCC's proposed § 15.11(b) codifies these requirements:

#	Reserve Asset Category	Key Characteristics and Constraints
1	United States coins and currency	Includes Federal Reserve notes. Limitations on transferability may warrant concentration limits (e.g., no more than 5–10% of reserves).
2	Demand deposits or insured shares at insured depository institutions	Subject to FDIC/NCUA insurance limits ($250K per depositor per institution). Uninsured portions carry credit risk. OCC proposes concentration limits per institution.
3	Treasury bills, notes, or bonds with remaining maturity ≤ 93 days	Subject to fair value (not amortized cost) valuation. Off-the-run securities may be less liquid and trade at a discount. OCC considering limits on notes/bonds vs. bills.
4	Money received under repurchase agreements (Treasuries)	Must involve Treasury collateral. Subject to the prohibition on rehypothecation of reserve assets.
5	Reverse repurchase agreements	Cleared, tri-party, or bilateral. Counterparty must be "adequately creditworthy even in the event of severe market stress." Subject to overcollateralization requirements.
6	SEC-registered money market fund shares	Must invest solely in other eligible reserve assets. Subject to look-through credit risk analysis. Must be redeemable "even in the event of severe market stress."
7	Other high-quality liquid assets (as determined by OCC)	Catch-all provision. OCC must determine that the asset is comparable in quality and liquidity to the other specified categories.
8	Tokenized forms of the above assets	Subject to OCC approval. The OCC proposes a case-by-case determination process. Introduces additional technology and legal risks requiring specific validation.

Critically, the proposed rule requires that these reserves be valued at fair value at all times, segregated from the issuer's other assets, identifiable with documented legal entitlement, and held either directly by the issuer or in custody at an eligible financial institution. The issuer is prohibited from pledging, rehypothecating, or reusing reserve assets, except for limited purposes such as earning interest on Treasury securities or satisfying redemption obligations.

1.5 Who Can Issue Payment Stablecoins?

The GENIUS Act generally prohibits any person other than a permitted payment stablecoin issuer from issuing a payment stablecoin in the United States. Three categories of entities may qualify as permitted payment stablecoin issuers: (1) subsidiaries of insured depository institutions (national banks, Federal savings associations, state banks, and credit unions) approved by their primary Federal regulator; (2) Federal qualified payment stablecoin issuers, which are non-bank entities chartered and supervised exclusively by the OCC; and (3) State qualified payment stablecoin issuers approved by their state regulator under a regime certified as substantially similar to the Federal framework. State qualified issuers with consolidated

outstanding issuance exceeding $10 billion must transition to the Federal regulatory framework within 360 days.

2. Risk Exposures for Financial Institutions

Financial institutions engaging in payment stablecoin activities—whether as issuers, custodians of reserve assets, or depository institutions holding stablecoin reserves—face a distinct set of risk exposures that differ in character and intensity from traditional banking risks.

2.1 Liquidity Risk

Liquidity risk is the paramount concern for stablecoin issuers, and the OCC's proposed rule reflects this priority throughout its provisions. Unlike bank depositors, stablecoin holders can initiate redemption requests 24/7/365 via blockchain transactions, creating the potential for rapid, large-scale outflows that far exceed the pace of traditional bank runs. Issuers must maintain the ability to monetize reserve assets quickly enough to satisfy redemption demand at par value.

This risk is amplified by the speed at which information travels in digital asset markets. Even a minor de-pegging event—where a stablecoin's secondary market price dips even slightly below $1.00—can trigger a cascade of algorithmic selling and manual redemptions within minutes. Unlike traditional bank deposits, where behavioral inertia and transaction friction slow withdrawal rates, stablecoin redemptions can be automated through smart contracts, removing human hesitation from the equation entirely.

The spring 2023 failure of Silicon Valley Bank provided a real-world demonstration of this dynamic. When it became known that Circle's USDC stablecoin held approximately $3.3 billion in reserves at SVB, USDC's secondary market price fell below $0.90, triggering billions of dollars in redemption requests over a weekend. The OCC's proposed rule explicitly references this event as motivation for its deposit diversification and liquidity requirements, noting the "potential knock-on effects of changes in interest rates and the importance of continuous monitoring for stablecoins, particularly if acute stress creates situations in which issuers are unable to access reserve assets."

2.2 Interest Rate Risk

Although reserve assets under the GENIUS Act are limited to short-duration instruments (93 days or less for Treasury securities), interest rate risk remains material for several reasons:

Reserve Fair Value Impact: Increases in interest rates reduce the fair value of fixed-income reserve assets, potentially creating shortfalls against the 1:1 backing requirement. Even with short maturities, rapid rate movements can create temporary fair value deficits that must be immediately remedied by adding additional reserves.

Earnings Vulnerability: Stablecoin issuers derive revenue primarily from interest earned on reserve assets. Changes in the yield curve—particularly inversions or sudden shifts—directly impact earnings. Since the GENIUS Act prohibits issuers from paying interest to stablecoin

holders, issuers benefit from higher rates but cannot pass through rate reductions, creating asymmetric risk to earnings sustainability.

Demand Sensitivity: Rising rates may reduce demand for non-interest-bearing stablecoins, as holders shift to interest-bearing alternatives (such as Treasury bills purchased directly, money market funds, or tokenized deposits that may pay interest). This could trigger redemptions and shrink the issuer's asset base.

The OCC draws explicit parallels to three money market fund failures caused by interest rate mismanagement, underscoring that even short-duration portfolios are not immune to rate-driven losses.

2.3 Credit Risk

Credit risk arises from multiple sources within the stablecoin reserve structure:

Uninsured Bank Deposits: Reserve assets held as deposits beyond FDIC insurance limits are subject to loss in the event of a depository institution failure. The OCC notes that a stablecoin with $1 billion in reserves, keeping 10% in bank deposits, would need to spread those deposits among 400 separate accounts to maintain full insurance coverage—a practical impossibility. As a result, most issuers will hold significant uninsured deposit balances, creating material counterparty credit exposure.

Reverse Repurchase Agreements: Bilateral reverse repo agreements expose issuers to counterparty default. In a default scenario, the issuer may receive long-dated Treasury securities (the GENIUS Act permits Treasury collateral with no maturity restriction for repos) with significant duration and price volatility. Even with overcollateralization, the price volatility of long-dated Treasuries could result in material losses.

Money Market Fund Look-Through Risk: Money market funds held as reserves invest in bank deposits and reverse repurchase agreements that carry the same counterparty risks as if held directly. The OCC notes that a capital framework may need to require issuers to "lock through to the underlying assets of the money market fund" to assess true credit exposure.

2.4 Operational Risk and Resilience

The OCC's capital framework focuses primarily on operational risk, recognizing it as the dominant risk category. The proposed rule further emphasizes that operational resilience—the ability to maintain stable value and continuous availability under adverse conditions—will be particularly important for stablecoin issuers to sustain customer confidence and systemic trust. Accordingly, the validation of custody, network, and disaster recovery models should be viewed not merely as risk management but as resilience testing, aimed at maintaining the stable value and availability required by the Act. The proposed rule identifies several key operational risk dimensions:

Technology and Smart Contract Failures: Smart contracts governing minting, burning, and transfers are software systems susceptible to coding errors, logic flaws, and exploits. The OCC references the PayPal/Paxos incident in October 2025, in which a technical error led to the minting of $300 trillion in stablecoins—a sum exceeding global GDP—as an illustration of the catastrophic potential of smart contract failures.

Private Key Management: Loss of, or unauthorized access to, private keys controlling stablecoin reserves or administrative functions could result in permanent, irrecoverable loss of digital assets. Unlike traditional banking systems where transactions can typically be reversed through institutional processes, blockchain transactions are generally irreversible.

Cross-Blockchain Transfer Risk: Payment stablecoins may operate across multiple distributed ledgers. Transferring stablecoins from one blockchain to another to satisfy a redemption demand introduces risks related to bridge technology, locking and minting mechanics, and settlement finality across different consensus mechanisms.

Cybersecurity: The OCC notes that a larger pool of underlying reserve assets "may increase the number and severity of hacking attempts," since the economic incentive for attackers scales with the value under management. Stablecoin issuers are high-value targets for sophisticated cyber adversaries.

Third-Party Dependency: Stablecoin operations depend on blockchain infrastructure providers, custodial technology platforms, oracle services (i.e., external data feeds that provide off-chain information such as asset prices to on-chain smart contracts), settlement systems, and key management vendors. Failure at any critical third-party provider can disrupt operations across the entire stablecoin lifecycle.

2.5 Concentration Risk

Concentration risk pervades stablecoin operations at multiple levels:

Deposit Concentration: Concentrating reserve deposits at a single insured depository institution creates correlated failure risk. The SVB-USDC episode demonstrated that reserve assets concentrated at a single institution can trigger a de-peg event affecting all stablecoin holders, even if the reserves at other institutions remain fully intact.

Custodial Concentration: Reliance on a single eligible financial institution for safekeeping of Treasury securities or repo collateral creates a single point of failure for asset access and monetization.

Counterparty Concentration: Dependence on a limited number of repo counterparties for monetization can constrain liquidity in stress scenarios precisely when it is most needed.

Blockchain Concentration: Operating on a single distributed ledger exposes the issuer to platform-specific risks, including network congestion, protocol upgrades that may disrupt functionality, or governance disputes that could fork the network.

2.6 De-Pegging and Run Risk

De-pegging occurs when a stablecoin's secondary market price diverges from its par value. This divergence can trigger a self-reinforcing cycle: the de-pegging signals potential solvency or liquidity problems, accelerates redemptions, and may force fire-sale liquidation of reserves at prices below fair value, which further depresses confidence in the peg.

The proposed rule addresses this risk through several mechanisms. First, reserve requirements are based on the par value of outstanding stablecoins (not their secondary market price), ensuring that issuers cannot reduce reserves when stablecoins trade below par. Second, surplus reserve withdrawals are restricted to periods following monthly examination and

certification, preventing issuers from removing excess reserves that may serve as a buffer during stress. Third, diversification and liquidity requirements are designed to ensure that issuers can meet redemption demands even during periods of market dislocation.

The OCC also asks in Question 86 whether additional measures should address de-pegging, recognizing that even well-designed reserve and liquidity frameworks may not fully prevent the behavioral dynamics that drive stablecoin runs.

3. The Model Risk Perimeter for Stablecoins

Model risk, as defined in the OCC's Bulletin 2011-12 and the Federal Reserve's SR 11-7, is the potential for adverse consequences arising from decisions based on incorrect or misused model outputs and reports. A model is defined as a quantitative method, system, or approach that applies statistical, economic, financial, or mathematical theories, techniques, and assumptions to process input data into quantitative estimates. The proposed GENIUS Act rulemaking creates an extensive model risk perimeter for permitted payment stablecoin issuers that financial institutions must identify, govern, validate, and monitor such models.

3.1 Taxonomy of Models in Stablecoin Operations

The following taxonomy identifies the principal model categories required for compliant stablecoin operations, mapped to the specific provisions of the OCC's proposed rule that create the regulatory mandate:

Model Domain	Model Examples	Regulatory Reference	Key Risk Factors
Reserve Valuation	T-bill pricing, repo valuation, money market fund NAV, tokenized asset pricing	§ 15.11(a)(1)(iii): Fair value of reserve assets must equal or exceed outstanding issuance value at all times	Discount rate assumptions, liquidity premiums, off-the-run spreads, tokenization premium/discount, continuous (24/7) valuation requirements
Liquidity Stress	Redemption outflow models, fire-sale discount models, monetization time models	Question 81; § 15.13(a)(8): Manage liquidity and concentration risk appropriate to business model	Scenario calibration with no regulatory-era historical data; tail distribution assumptions; correlation of redemptions with market stress; 24/7 redemption dynamics
Interest Rate Risk	Duration/convexity models, NII sensitivity projections, EVE analysis	§ 15.13(a)(3): Manage IRR appropriate to size, complexity, and composition of assets and liabilities	Yield curve modeling; earnings sensitivity given no interest pass-through to holders; demand elasticity to rate changes; deposit behavior assumptions
Capital Adequacy	ICAAP-style projections, operational risk	§ 15.41(a)(2): Assess capital commensurate with business model	Revenue projections under novel business model; expense volatility; operational loss

	quantification, multi-scenario capital planning, 12-month operating expense forecasting (burn rate models)	and risk profile, incorporating loss from all sources	distribution tail assumptions; limited operating history; burn rate model understating costs triggers capital shortfall against 12-month backstop
Concentration Risk	Portfolio optimization, counterparty exposure analytics, HHI calculations	§ 15.11(c): Diversification and concentration requirements (Option A safe harbor or Option B mandatory)	Multi-constraint optimization (yield, coverage, diversification, WAM, liquidity); correlation assumptions; safe harbor vs. principles-based compliance
Operational Risk and Resilience	Loss distribution models, scenario-based OpRisk, key risk indicator frameworks	§ 15.41 (capital focused on OpRisk); § 15.13(a)(1): Effective risk assessment	Emerging risk category with sparse loss data; cyber and smart contract failure modes; scaling risk with issuance growth; cross-blockchain operational risk
Smart Contract Validation	Algorithmic control validation, minting/burning logic verification, access control testing	§ 15.13(b)(3)(iii): Evaluate and validate that IT systems and smart contracts operate as intended	Novel “model” category; code-as-model paradigm where errors execute autonomously; upgrade and migration risks; oracle dependency; boundary conditions
Monetization Capability	Liquidation cost models, market depth analysis, time-to-monetize estimation, execution risk models for mandatory monetization testing	§ 15.11(a)(2): Demonstrate operational capability to access and monetize reserve assets	Stress-conditional liquidity assumptions; repo market depth under correlated stress; signaling effects of monetization channel usage; fire-sale dynamics; demonstration slippage between theoretical and actual execution prices during mandatory regulatory tests

3.2 What Makes Stablecoin Model Risk Unique

Stablecoin model risk differs from traditional banking model risk in several important dimensions that institutions must account for in their model risk management frameworks:

24/7 Operational Exposure: Unlike traditional financial markets, which operates within defined trading hours and settlement windows, stablecoin redemptions and transfers operate continuously across global time zones. Models must function and remain valid around the clock, without interruption. Valuation models must produce fair values on weekends and holidays, when traditional bond markets are closed. Liquidity stress models must account for the possibility that a run could begin at 2 a.m. on a Saturday.

Limited Historical Data: Payment stablecoins operating under the GENIUS Act regulatory framework have no operating history under these specific regulatory conditions. Models cannot be calibrated to historical regulatory-era data, increasing reliance on theoretical frameworks,

analogous instruments (money market funds, prime brokerage operations), expert judgment, and stress scenarios. Traditional backtesting approaches will initially have very short observation windows, requiring supplementary validation techniques.

Technology-Embedded Models: Smart contracts represent a paradigm shift in model risk. They are themselves models—algorithmic decision-making systems that process inputs and produce outputs—but unlike traditional quantitative models, which inform human decisions, smart contracts execute decisions autonomously on the blockchain. A pricing model error in a traditional bank produces a report that a human reviews before acting. A smart contract error executes immediately, potentially minting billions of tokens (as in the PayPal/Paxos incident) or freezing legitimate transactions. This tighter coupling between model error and financial consequence demands a higher standard of pre-deployment validation.

Rapid Contagion Dynamics: Digital asset markets transmit information faster and exhibit more correlated behavior than traditional financial markets. Social media, on-chain analytics, and automated trading algorithms can propagate a de-pegging signal globally within minutes. Models must account for the speed at which redemption cascades develop, as well as the potential for cross-stablecoin contagion, where the failure or de-pegging of one stablecoin triggers runs on other stablecoins perceived to have similar risk characteristics.

Regulatory Novelty: The GENIUS Act framework is unprecedented. There is no established body of supervisory expectations, examination findings, or enforcement actions to guide model development. Institutions must build models that anticipate regulatory expectations, rather than responding to established precedent. As the OCC itself acknowledges, it "anticipates that these implementing regulations will be updated, as necessary, in the years following the effective date."

4. A Framework for Managing Stablecoin Model Risk

The following framework draws on the principles of OCC Bulletin 2011-12 (SR 11-7) and adapts them to the specific characteristics of payment stablecoin operations under the GENIUS Act. It is designed to be scalable—applicable to both smaller de novo issuers and larger, more complex institutions—while remaining consistent with the OCC's principles-based approach in proposed § 15.13.

4.1 Governance Structure

Effective model risk governance for stablecoin issuers requires several foundational elements:

Board Oversight: The board of directors (or an appropriate board committee) must understand the model risk inherent in stablecoin operations and receive regular reporting. This aligns with proposed § 15.13(a)(3), which requires board reporting on interest rate risk, and the broader expectation in § 15.13(a)(2) for board review of internal audit effectiveness. Board reporting should include the status of the model inventory, outstanding validation findings, model performance metrics, and any material model failures or breaches.

Model Inventory: A comprehensive model inventory must capture not only traditional quantitative models, such as valuation, stress testing, capital, but also smart contracts, algorithmic controls, and technology-embedded decision systems. Each model should be

documented with its purpose, owner, inputs, outputs, assumptions, limitations, and validation status. The inventory should distinguish between models that inform decisions and models that execute decisions (smart contracts), given the different risk profiles of each.

Risk Tiering: Models must be tiered based on their risk significance. For stablecoin operations, risk tiering for stablecoin models should reflect the unique characteristics of the business: smart contracts governing minting and burning operations should receive the highest-tier classification given their autonomous execution and catastrophic failure potential; reserve valuation and liquidity stress models should be high-tier because of their direct impact on the 1:1 backing requirement; and supporting models, such as concentration analytics, reporting tools, may be assigned lower tiers with correspondingly lighter validation requirements.

Three Lines of Defense: While the proposed rule explicitly states that it "would not mandate a particular organizational structure (for example, three lines of defense)," it requires functionally equivalent capabilities: business-line model ownership and first-line controls, independent model validation, and internal audit oversight. Smaller issuers may satisfy these requirements through outsourced validation and audit functions, as the proposed rule permits.

4.2 Model Development Standards

Given the limited historical data available for stablecoin operations under the GENIUS Act framework, model development must place heightened emphasis on several areas:

Theoretical Soundness: In the absence of robust historical data, the conceptual foundation of each model becomes proportionally more important. Development documentation should demonstrate that the model's theoretical framework is appropriate for the specific risk being measured and that its assumptions are defensible in the stablecoin context.

Benchmarking Against Analogous Instruments: Stablecoin reserve portfolios share characteristics with money market funds, treasury management operations, and prime brokerage cash management. Calibrating models to the historical behavior of these analogous products—while documenting the differences and additional risks specific to stablecoins—provides a reasonable starting framework.

Expert Judgment Protocols: When data is insufficient for statistical estimation, models will necessarily incorporate expert judgment. Institutions should establish formal protocols for eliciting, documenting, and challenging expert assumptions, including the range of reasonable alternatives considered and the rationale for the selections made.

Comprehensive Sensitivity Analysis: Every model should be subjected to sensitivity analysis across a wide range of input assumptions to identify which parameters most materially affect outputs. This is particularly important for models with limited empirical calibration, as it reveals the degree of uncertainty in model results.

4.3 Independent Model Validation

The proposed rule's requirements for internal audit and independent review (§ 15.13(a)(2)) create a clear mandate for independent model validation. The OCC's existing guidance on model risk management calls for "effective challenge" of models by parties independent of the model development process. For stablecoin issuers, validation activities should encompass four core pillars:

Conceptual Soundness Assessment: Evaluate whether the theoretical framework of each model is appropriate for stablecoin-specific risks. This includes assessing whether valuation models properly account for the liquidity characteristics of different reserve asset types, whether stress scenarios adequately reflect the speed and magnitude of stablecoin-specific events, such as 24/7 redemptions, contagion effects, and whether smart contract logic correctly implements the intended business rules and compliance controls.

Outcomes Analysis: Compare model predictions to actual results on an ongoing basis. For stablecoin models, backtesting windows will initially be very short, requiring supplementary techniques such as benchmarking against analogous products, out-of-sample testing on simulated data, and comparison to alternative modeling approaches.

Process Verification: Confirm that model inputs, calculations, and outputs are implemented correctly. For smart contracts, this extends to code review, formal verification (mathematical proofs of correctness), and testing across boundary conditions. For quantitative models, this includes replication of calculations and verification of data feeds.

Ongoing Monitoring: Establish performance metrics and thresholds that trigger re-validation when breached. For reserve valuation models, this might include tracking the difference between model-predicted fair values and observed transaction prices. For liquidity stress models, this might include monitoring actual redemption patterns relative to model-predicted distributions.

For de novo stablecoin issuers that lack internal validation resources, engaging qualified third-party validation firms is essential. The OCC's existing guidance permits outsourcing of validation functions, and the proposed rule explicitly acknowledges that smaller issuers "may be able to outsource certain functions such as the internal audit function" (§ 15.13(a)(2) supplementary information).

Distinguishing External Audit from Model Validation: The proposed rule requires that a registered public accounting firm randomly select one day each month to report on reserve composition and adequacy (§ 15.11(e)–(f)). While this external audit confirms that reserves exist and are properly valued on a given date, it does not assess whether the valuation models themselves are conceptually sound, correctly implemented, or performing within acceptable tolerances. Institutions must clearly delineate the boundary between the financial audit of reserves and the model validation of the valuation engines, stress-testing frameworks, and risk quantification tools that produce the numbers auditors examine. The MRM function should leverage the auditor's monthly randomized reports as an independent data source for outcomes analysis—comparing model-predicted valuations against auditor-confirmed values—while recognizing that audit and validation serve fundamentally different purposes, and neither substitutes for the other.

4.4 Stress Testing Framework

A robust stress testing framework for stablecoin model risk should incorporate multiple, complementary dimensions of stress. Institutions should design scenarios that reflect the specific vulnerabilities identified in the proposed rule:

Liquidity Stress: Model rapid, large-scale redemption scenarios at multiple severity levels. Consider scenarios in which 20–50% of outstanding stablecoins are tendered for redemption within 24–48 hours. Assess the ability to monetize reserve assets under each scenario, including time-to-monetization, fire-sale discounts, and the availability of repo counterparties

under stress conditions. Liquidity stress scenarios should also incorporate cross-border settlement risk: stablecoins operate globally on a 24/7 basis, whereas U.S. Treasury markets, repo facilities, and bank settlement systems observe business hours and holidays. Models that assume continuous monetization capability contain a conceptual soundness flaw when the stablecoins are held or redeemed across time zones where settlement bridges are closed. Stress tests should explicitly model time-zone mismatch scenarios and cross-border settlement lags, particularly during peak redemption periods that coincide with U.S. market closures.

Market Stress: Test reserve asset valuations under severe interest rate shocks (e.g., 100–300 basis point parallel shifts within one week), Treasury market dislocations affecting bid-ask spreads and market depth, and repo market freezes in which counterparties decline to roll existing agreements or enter new ones.

Monetization Testing and Demonstration Slippage: The proposed rule requires issuers to demonstrate operational capability to monetize reserve assets. The OCC acknowledges that monetization testing—selling assets solely to prove they can be sold—may force institutions to recognize a loss for a sale conducted purely for demonstration purposes. This introduces demonstration slippage: the measurable difference between a theoretical mid-market price and the actual execution price during a forced regulatory test. Valuation and execution risk models must account for this slippage, which may be particularly material during periods of market stress or illiquidity. Validation should confirm that models incorporate realistic execution costs for mandatory test windows and that demonstrated monetization capacity is not overstated by models calibrated only to normal market conditions.

Operational Stress: Model the impact of smart contract failures (unauthorized minting, frozen redemptions), cybersecurity breaches compromising private keys or administrative access, and key management vendor failures disrupting the ability to execute transactions on the blockchain.

Concentration Stress: Test the simultaneous failure of the largest custodian, the largest depository institution holding reserves, or the largest repo counterparty. The SVB-USDC event provides a historical calibration point for this type of scenario.

Capital Adequacy Stress: The OCC's proposed capital framework includes a 12-month operating expense backstop—requiring issuers to maintain capital sufficient to cover projected operating costs for twelve months even in the absence of revenue. The burn rate model used to forecast these expenses becomes a Tier 1 model, as underestimation directly results in failure to meet the minimum capital requirement. Stress testing should subject expense projections to scenarios including accelerated technology spending, increased compliance costs, elevated legal expenses, and revenue disruption. Institutions should validate that the burn rate model captures the full cost structure of 24/7 stablecoin operations, including blockchain infrastructure, cybersecurity, and the operational resilience investments required under the proposed rule.

Contagion Stress: Model the impact of another stablecoin's failure or de-pegging event on redemption demand for the issuer's own stablecoin. Cross-stablecoin contagion is a systemic risk that the proposed rule acknowledges but does not fully address. Institutions should self-impose stress scenarios reflecting this risk.

4.5 Smart Contract Validation Methodology

Smart contract validation represents a novel extension of traditional model validation methodology that institutions must develop or acquire. An effective smart contract validation approach should include:

Code Review and Formal Verification: Apply mathematical proof techniques to verify that contract logic produces correct outcomes under all possible input conditions. Formal verification goes beyond testing (which can only prove the presence of bugs) to provide mathematical assurance of correctness within defined parameters. This is particularly important for minting and burning functions where errors can have immediate, large-scale financial consequences.

Boundary Testing: Verify smart contract behavior at extreme inputs, including zero balances, maximum supply scenarios, simultaneous high-volume transactions, integer overflow and underflow conditions, and interactions between multiple concurrent transactions that may create race conditions.

Upgrade and Migration Testing: When smart contracts are upgraded or migrated to new blockchains, validation must confirm that all functionality is preserved and no new vulnerabilities are introduced. The proposed rule contemplates that issuers may operate across multiple distributed ledgers, making migration testing a recurring requirement.

Oracle Dependency Analysis: Assess the reliability and resistance to manipulation of any external data feeds (oracles) that smart contracts rely on for pricing, rate, or other inputs. Oracle manipulation is a well-documented attack vector in decentralized finance, and reserve valuation processes that depend on oracle feeds require specific risk assessment.

Access Control Verification: Confirm that administrative functions (pause, freeze, upgrade, emergency shutdown) can only be exercised by authorized parties under appropriate conditions, with proper logging and alerting. Verify that no single individual can unilaterally execute critical administrative functions (multi-signature requirements).

Compliance Logic Validation: The OCC solicits comment on whether to mandate technical requirements through smart contracts, including regulatory wrappers that embed compliance logic directly in contract code—for example, automatically freezing funds to comply with court orders, restricting transfers to non-KYC'd wallets, or enforcing sanctions screening at the protocol level. This compliance logic introduces a distinct model risk vector: if freeze logic is flawed, the issuer faces legal liability for failing to comply with lawful orders; if it triggers erroneously, it can cause reputational damage and operational disruption. Validation of compliance logic should include legal requirement traceability (confirming each automated rule maps to a specific regulatory obligation), false positive and false negative testing under realistic transaction volumes, jurisdictional conflict analysis for cross-border operations, and regression testing following any updates to compliance rules or underlying regulatory requirements.

4.6 Ongoing Monitoring and Reporting

The continuous, 24/7 nature of stablecoin operations demands monitoring capabilities that exceed traditional banking standards. The proposed rule's reporting requirements—weekly data submissions (§ 15.14(h)), monthly examination and public certification (§ 15.11(e)–(f)), and quarterly financial reports (§ 15.14(i))—establish a baseline. However, effective model risk monitoring should go further:

Daily Reserve Coverage Verification: Conduct automated comparison of the fair value of all reserve assets to the outstanding issuance value, with immediate alerts when the coverage ratio approaches or breaches 1:1. This monitoring must operate continuously and account for intraday movements in both reserve fair values and stablecoin issuance.

Real-Time Peg Monitoring: Track the stablecoin's secondary market price across all exchanges and trading venues, with tiered alerts when deviations exceed defined thresholds (e.g., 0.1%, 0.5%, 1.0%). Significant de-pegging events should trigger pre-defined escalation and response protocols.

Redemption Pattern Analysis: Analyze redemption volumes, velocity, and patterns to identify early indicators of emerging run risk. Statistical models can identify abnormal redemption activity relative to historical baselines and flag potential stress events before they fully materialize.

Model Performance Dashboards: Provide senior management and the board with timely information on model accuracy, breaches, validation findings, and remediation status. Dashboards should highlight any models operating outside approved parameters or with outstanding material findings.

Regulatory Reporting Automation: Implement systems to support the weekly data submissions required under proposed § 15.14(h)—covering outstanding issuance value, reserve assets, redemptions, minting, exchange listings, concentration data, securities details, and repo information—as well as the monthly public disclosures and quarterly financial reports.

5. Regulatory Outlook and Preparedness

The GENIUS Act's effective date is the earlier of 18 months after enactment (January 18, 2027) or 120 days after the primary Federal payment stablecoin regulators issue final regulations. With the OCC's NPRM now published and final rules required by July 18, 2026, institutions considering stablecoin issuance face a defined—and compressed—timeline for preparedness.

5.1 Immediate Priorities (Now – Q2 2026)

1. Perform a comprehensive risk assessment of planned stablecoin activities, identifying all model dependencies across the eight domains described in this paper.
2. Build a preliminary model inventory capturing all quantitative and algorithmic decision-making systems required for compliant operations.
3. Engage independent validation for the highest-risk models, particularly reserve valuation, liquidity stress, and smart contract logic, well in advance of the OCC's final rule.
4. Submit comments on the proposed rule to influence the final requirements in areas affecting model risk management.

5.2 Medium-Term Priorities (Q3 2026 – Q1 2027)

1. Develop an enterprise model risk management framework aligned with OCC 2011-12 / SR 11-7 principles, tailored to stablecoin-specific risks and the final rule's requirements.
2. Implement technology platforms to support model governance, monitoring, and the proposed rule's weekly, monthly, and quarterly reporting obligations.

3. Build or acquire internal capabilities for smart contract validation and blockchain risk assessment.
4. Establish stress testing programs incorporating the multi-dimensional scenarios described in Section 4.4.

5.3 Longer-Term Considerations (2027 and Beyond)

1. Prepare for the OCC's stated intention to evolve toward "more standardized, objective capital requirements" as the industry matures and issuers establish longer operating histories.
2. Anticipate additional rulemaking by the Treasury, FDIC, Federal Reserve, NCUA, and state regulators under their respective GENIUS Act authorities.
3. Monitor the development of interoperability standards under Section 12 of the GENIUS Act, which may introduce new model requirements for cross-platform operations.
4. Accumulate operational data to improve model calibration, replacing initial theoretical and expert-judgment-based assumptions with empirical estimates as regulatory-era experience develops.

Conclusion

The GENIUS Act and the OCC's implementing regulations represent both a landmark regulatory achievement and a significant new frontier for model risk management. Payment stablecoins introduce model risk exposures that are familiar in concept—such as valuation, liquidity, interest rate, credit, and operational risk models—but novel in their specific characteristics: continuous 24/7 operations, technology-embedded autonomous decision-making, limited historical data, and rapid contagion dynamics.

Financial institutions that build robust, well-governed model risk management frameworks from inception will be best positioned to operate safely and competitively in this new regulatory environment. Those that treat model risk as an afterthought will face not only regulatory challenges during the OCC's examination process but also the material financial risks that the GENIUS Act is designed to mitigate.

The framework presented in this paper—covering governance, development standards, independent validation, stress testing, smart contract validation, and ongoing monitoring—provides a practical starting point for institutions entering or expanding in the payment stablecoin space. It is designed to be adapted and refined as the regulatory framework evolves, operational data accumulates, and the industry matures.

How Kevin D. Oden & Associates Can Help

Kevin D. Oden & Associates LLC (KDOA) brings nearly eight years of specialized experience and has completed over 500 client engagements in model risk management, quantitative analytics, and regulatory advisory for financial institutions. Our expertise positions us to support institutions across the full spectrum of stablecoin-related model risk challenges:

Independent Model Validation: KDOA provides rigorous validation of reserve valuation models, liquidity stress tests, interest rate risk models, capital adequacy frameworks, and operational risk quantification models fully compliant with OCC 2011-12 / SR 11-7 Our quantitative depth—rooted in advanced stochastic calculus and mathematical finance—enables us to evaluate the complex models required for stablecoin operations.

MRM Framework Design: For de novo stablecoin issuers building risk infrastructure from the ground up, KDOA designs and implements end-to-end model risk management frameworks tailored to the unique characteristics of payment stablecoin operations—including model inventories that capture both traditional quantitative models and technology-embedded systems, such as smart contracts.

Regulatory Readiness and Gap Analysis: KDOA performs comprehensive assessments comparing current practices against the proposed rule's requirements for capital adequacy, reserve management, risk governance, and information security, delivering prioritized remediation roadmaps to support charter applications and examination preparedness.

Smart Contract and Technology Risk Assessment: KDOA extends proven model validation methodologies to the algorithmic controls embedded in smart contracts—including minting and burning logic, access controls, oracle dependencies (i.e., external data feeds that provide off-chain information such as asset prices to on-chain systems), and cross-chain bridge risks.

Model IQ Platform: KDOA's proprietary Model IQ software platform provides the technology infrastructure to manage model inventories, track validation findings, monitor model performance, and produce the regulatory reporting required under the proposed rule's weekly, monthly, and quarterly obligations. For de novo issuers, Model IQ can serve as the foundational model risk management system from day one.

Whether your institution is exploring a stablecoin charter, establishing a stablecoin-issuing subsidiary, or serving as a custodian or depository for stablecoin reserve assets, KDOA offers the combination of regulatory expertise, quantitative rigor, and purpose-built technology to help you navigate this new landscape with confidence.

KEVIN D. ODEN
& ASSOCIATES

About Kevin D. Oden & Associates LLC

Kevin D. Oden & Associates LLC (KDOA) is a San Francisco-based consulting firm specializing in model risk management and quantitative analysis for financial institutions. Founded nearly eight years ago, KDOA has completed over 500 client engagements spanning model validation, risk management advisory, and regulatory compliance under frameworks including OCC Bulletin 2011-12 (SR 11-7). The firm's team brings deep expertise in stochastic calculus, mathematical finance, and advanced quantitative methods to complex risk management challenges.

In Q3 2025, KDOA launched Model IQ, a proprietary model risk management software platform designed to support the full lifecycle of model governance, validation, and monitoring. Model IQ provides financial institutions with the technology infrastructure needed to manage model inventories, track validation findings, monitor model performance, and produce regulatory reporting.

KDOA stands ready to support financial institutions in navigating the GENIUS Act's model risk landscape with the quantitative rigor, regulatory expertise, and practical orientation that effective model risk management demands.

Contact

Kevin D. Oden, PhD

Founder & Principal

Kevin D. Oden & Associates LLC

San Francisco, California

info@kdoa.com

www.kdoa.com