Deloitte.

Together makes progress

Implementing GENIUS: Risk management considerations

April 2026

Center *for*
Regulatory Strategy US

GENIUS Act rulemaking reflects heightened regulatory expectations for risk management

What is the GENIUS Act?

Enacted in July 2025, the GENIUS Act establishes the core US federal regulatory framework for payment stablecoins and limits issuance to permitted payment stablecoin issuers, including federally-approved nonbank issuers, federally-approved bank subsidiaries, state-qualified issuers operating under a certified "substantially similar" state regime, and registered foreign issuers.[1] Oversight is split across multiple regulators, principally the federal banking regulators, Department of the Treasury, and relevant state regulators, depending on issuer type and scale. As of April 2026, implementing regulations of the GENIUS Act are under active proposed rulemaking.[2]

Why GENIUS Act implementation is a risk-management problem

Payment stablecoins are moving from niche crypto use toward mainstream payment and treasury use cases, which raises the bar on day-to-day controls and supervisory readiness. The GENIUS Act sets clearer "trust rules" such as one-to-one reserves in high-quality liquid assets, segregation/limitations on reserve use, monthly reserve disclosures, and a ban on paying yield to holders. Issuers should plan now for requirements to take effect on the statutory timeline tied to rulemaking (18 months after enactment or earlier depending on final rules).

Core risk management considerations

As stablecoin regulation moves toward a more bank-like prudential supervisory posture, the core risk management considerations below should be read as a program uplift, not a set of one-off controls. This is especially true for entities that are newly subject to state oversight and for federally regulated trust banks, where expectations typically align to established banking standards for governance, controls, monitoring, and evidence production. In practice, that means reinforcing a clear three-line model, tightening continuous monitoring and escalation routines, and designing controls to be operationally scalable and auditable from day one. Because stablecoin operations can be high-velocity and irrevocable, leading organizations should also prioritize automation of key workflows (e.g., reconciliations, access governance, exception handling) to reduce manual error and improve response speed under stress. The following are considerations that stablecoin issuers may incorporate into their operating framework:

Governance and operating model: Clarify who is accountable for reserves, issuance, compliance, and customer outcomes across the issuer and partners. Unclear or overlapping responsibilities can delay decisions, weaken controls, and create inconsistent customer and regulator responses.

Risk and controls: Define a clear risk appetite and supporting key risk indicators (KRIs) (e.g., reconciliation break thresholds, redemption service level agreements [SLAs], key-operations exceptions) with mandatory management actions when breached. Post-launch vulnerabilities often arise when controls weaken over time, including ineffective independent testing, unclear remediation ownership, and insufficient issue closure. Special emphasis could be placed on trust bank-specific processes and controls rather than enterprise-wide ones.

Operational backstop and reserve segregation: Business continuity and recovery should be supported by a dedicated pool of highly liquid assets, held separately from the one-to-one reserve assets backing outstanding stablecoins. This structure helps the issuer sustain critical operations during a disruption without comingling or depleting assets reserved for redemption.

Reserve management: Establish a reserve operating model with eligibility rules, controls to facilitate segregation over movements, intraday reconciliation, independent pricing and valuation controls, and repeatable disclosure support. A potential risk is reconciliation breaks, liquidity shortfalls under stress, or reporting inaccuracies which can impair timely redemptions and supervisory confidence.

Mint and burn: Implement policy-driven issuance and redemption workflows with hard caps. A key risk is an unauthorized or erroneous mint or burn (or parameter/configuration drift) that may create a solvency or confidence shock.

Key management: Operate an audited key-management life cycle (generation, activation, rotation, backup, recovery, destruction) with least-privilege access controls, strong approval gates, and continuous monitoring of privileged actions. Use hardened custody architectures (e.g., air-gapped hardware security module [HSM] and/or multi-party computation [MPC]) with quorum enforcement and tightly governed break-glass procedures to reduce compromise and insider-risk blast radius.

IT, cyber, and operational resilience: Operate bank-grade technology and cybersecurity environments that are resilient to outages, cyber incidents, and third-party disruptions, and that support continuous stablecoin issuance, reserve management, and timely redemption. The proposed rulemakings signal regulatory expectations that issuers maintain strong access controls, disciplined change management, monitoring, incident response, and recovery capabilities commensurate with the criticality of stablecoin operations. Technology failures or cyber events, particularly those affecting issuance systems, reserve operations, or redemption processing, can disrupt core obligations under the GENIUS Act framework and quickly escalate from an operational incident to a supervisory concern.

Third parties: Bring critical third-party providers into an end-to-end process and control framework, and support this by establishing explicit contractual rights to audit and perform sample testing. Mitigate risk through measurable KRIs, fourth-party transparency, and validated relationship exit plans. Risks can emerge where a vendor outage or control weakness disrupts operations and prevents the organization from demonstrating compliance in a timely manner.

KYC/AML: Align responsibilities between the issuer and distributors for know your customer (KYC), anti-money laundering (AML), sanctions screening, transaction monitoring, investigations, and escalation actions with a single-case system-of-record. A potential risk is channel fragmentation (data gaps, inconsistent rules, delayed Suspicious Activity Report [SAR] decisions) that may drive enforcement exposure and reputational harm.

Operations and change management: Enforce disciplined configuration management practices (e.g., tested deployments, approvals, environment parity, controlled allowlists, and rollback plans) with operational runbooks and reconciliations treated as key controls. Organizations should be cautious of rushed change risk, which may introduce outages or control bypasses, especially when scaling to multiple chains, partners, and products.

Monitoring and incident response: Implement layered monitoring (on-chain, off-chain, infrastructure, fraud, AML, and reserve operations) with severity models, on-call coverage, playbooks, and post-incident root-cause remediation tracking. A key risk is alert fatigue and slow containment, which can turn a manageable control failure into a market-wide confidence event.

Where to go from here

GENIUS Act implementation will hinge on day-to-day operating discipline, so immediate objectives should be to stand up an integrated program that converts statutory requirements into processes that are end-to-end and controls that are clearly owned, continuously monitored, and demonstrably effective and risks identified.

Organizations should start by establishing clear accountability for reserves, issuance, compliance, and customer outcomes across the issuer and its partners, and then translate those requirements into measurable standards for redemption performance, reserve integrity, key management, monitoring, escalation, and change control that can keep pace with stablecoin operations.

A digital asset risk assessment, together with legal interpretation and supervisory expectations, can help organizations manage the risks that can break redemption confidence or supervisory trust, and strengthen the controls associated with those risks first. It is important to build an audit-ready evidence backbone from the start, so disclosures, attestations, exceptions, and incidents are consistently captured and defensible under examination.

Finally, organizations should be prepared to validate readiness through realistic stress scenarios and independent testing so inevitable events may remain contained and managed, rather than escalate into broader market confidence issues. A targeted readiness sprint can quickly turn these considerations into a prioritized roadmap, a minimum viable control baseline, and an execution backlog aligned to the chosen stablecoin model.

APPENDIX 1: OCC is actively seeking feedback on its risk management approach

In the proposed rule, the Office of the Comptroller of the Currency (OCC) devotes 15+ questions, summarized below, seeking feedback on whether its proposed, principles-based risk management framework requirements appropriately capture the risks of stablecoin issuance and whether additional clarity, tailoring, or safeguards are needed to ensure safe and sound operations as the market scales. The comment period deadline is May 1, 2026.

Themes	Considerations
Scope and proportionality of risk-management frameworks	Whether the proposed risk-management requirements are appropriately scaled to issuer size, complexity, and business model, including for nonbank trust banks and newly formed entities.
Governance, accountability, and control ownership	How issuers should evidence clear accountability for risk management, including the role of boards and senior management in overseeing stablecoin issuance, reserves, and redemption activities.
Operational risk and resilience	Whether the proposed framework sufficiently addresses operational risks inherent in stablecoin issuance, including technology dependencies, system outages, cyber events, and third-party service provider failures.
Issuance, redemption, and liquidity risk	The effectiveness of proposed risk-management expectations in supporting timely redemption at par under normal and stressed conditions, and whether additional guardrails or stress considerations should apply.
Reserve management and safeguarding	Whether the proposed approach to reserve asset controls, segregation, monitoring, and reporting is sufficient from a risk-management perspective, or whether additional requirements are needed to mitigate operational or market risk.
Third-party and outsourcing risk	How risk-management expectations should apply where critical activities (e.g., custody, technology, transaction processing) are performed by affiliates or external service providers.
Interaction with capital and operational backstops	Whether the overall package appropriately mitigates risk, including the liquidity-vs-capital / buffer design trade-offs discussed in the proposal.
Compliance and incentive risks	Whether consumer protection and data privacy compliance standards, and compensation-related safeguards should be included.

Endnotes

1. Guiding and Establishing National Innovation for US Stablecoins (GENIUS) Act, 119th Cong., Pub. L. No. 119-27 (2025).
2. Office of the Comptroller of the Currency (OCC), "Implementing the Guiding and Establishing National Innovation for U.S. Stablecoins Act for the Issuance of Stablecoins by Entities Subject to the Jurisdiction of the Office of the Comptroller of the Currency," *Federal Register*, March 2, 2026; Federal Deposit Insurance Corporation (FDIC), "GENIUS Act Requirements and Standards for FDIC-Supervised Permitted Payment Stablecoin Issuers and Insured Depository Institutions," *Federal Register*, April 10, 2026.

Contact us

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

Joshua Flyer
Senior Manager
Deloitte & Touche LLP
jflyer@deloitte.com

Raquel Look
Senior Manager
Deloitte & Touche LLP
rlook@deloitte.com

Jann Futterman
Senior Manager
Deloitte & Touche LLP
jfutterman@deloitte.com

Richard Mumford
Independent Senior Advisor to
Deloitte & Touche LLP
rmumford@deloitte.com

David Hunter
Independent Senior Advisor to
Deloitte & Touche LLP
dahunter@deloitte.com

Arpita Mukherjee
Senior Solution Manager
Deloitte & Touche Assurance and Enterprise Risk Services India Private Limited
arpimukherjee@deloitte.com

CJ Burke
Manager
Deloitte & Touche LLP
cjburke@deloitte.com

Ellen Boyer
Manager
Deloitte & Touche LLP
eboyer@deloitte.com

Austin Parmer
Senior Consultant
Deloitte & Touche LLP
aparmer@deloitte.com

Deloitte Center for Regulatory Strategy, US

Irena Gecas-McCarthy
FSI Director, Deloitte Center for Regulatory Strategy, US
Principal
Deloitte & Touche LLP
igecasmccarthy@deloitte.com

Aaron Salerno
Manager
Deloitte Services LP
asalerno@deloitte.com

Kyle Cooke
Manager
Deloitte Services LP
kycooke@deloitte.com

Deloitte.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

About Deloitte

As used in this publication, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2026 Deloitte Development LLC. All rights reserved.