Stablecoin Readiness Self-Assessment

How to use this document

This self-assessment is a 15-question instrument across five dimensions of stablecoin readiness. Each question has three maturity tiers. Score honestly. The most useful outcome from this exercise is the gap between where the institution sits today and where it needs to sit before the first stablecoin-related vendor engagement or customer-facing product launch.

The five dimensions:

1. Governance and Strategy
2. Treasury and Reserve Custody
3. Technology and Blockchain Operations
4. Third-Party and Fourth-Party Risk Management
5. Customer-Facing and Frontline

For each question, circle the tier (1, 2, or 3) that most accurately describes the institution's current state. Tier 1 (Not Ready) means the capability is not yet in place. Tier 2 (Foundational) means it is partially in place and being built out. Tier 3 (Operating) means it is fully in place, documented, and operating effectively. The scoring section at the end aggregates the result into a readiness profile.

This instrument is designed for the institution's internal use. It does not need to be shared with regulators, vendors, or third parties. The honest score is the useful score.

Dimension 1. Governance and Strategy

Question 1.1. Board-approved risk appetite for digital-asset activities

- **Tier 1 (Not Ready).** The board has not addressed digital-asset activities. The institution does not have a documented position on stablecoins, on-chain custody, or any related activity.
- **Tier 2 (Foundational).** The board has discussed digital-asset activities at least once in the past 12 months and has documented a position (proceed, defer, decline) in the board minutes. A written risk-appetite statement covering digital-asset activities exists but has not been refreshed in the current planning cycle.
- **Tier 3 (Operating).** The board has approved a written digital-asset risk appetite statement within the current planning cycle, the statement specifies the activities the institution will and will not pursue, the statement is referenced in the institution's enterprise risk management framework, and the next refresh cadence is calendared.

Question 1.2. Strategic plan integration

- **Tier 1.** Stablecoins and digital-asset activities do not appear in the institution's current strategic plan or three-year financial projections.
- **Tier 2.** The strategic plan acknowledges stablecoin and digital-asset activities as a topic to monitor, but no specific revenue or activity targets have been set. The chief financial officer has not modeled the impact on net interest margin or fee income.
- **Tier 3.** The strategic plan addresses stablecoin activities as a defined revenue line or strategic position. The chief financial officer has modeled at least one scenario (reserve-deposit custody, reciprocal-deposit redistribution, or validator revenue) with documented assumptions. The chief executive officer can articulate the institution's position to a regulator, a correspondent banker, and a board member.

Question 1.3. Policy and procedure coverage

- **Tier 1.** Existing policies (BSA/AML, third-party risk management, information security, customer identification) do not address digital-asset activities. The institution would need to draft new policy language before opening any vendor file.
- **Tier 2.** Existing policies have been amended to add digital-asset language, but the amendments have not been examined or formally adopted by the board.
- **Tier 3.** The board has adopted policy amendments addressing digital-asset activities, the amendments cite the relevant regulatory anchors (GENIUS Act, CLARITY Act, OCC Interpretive Letters 1172, 1174, 1183, 1184, FDIC FIL-7-2025), and the amendments have been reviewed in the institution's most recent compliance audit.

Dimension 2. Treasury and Reserve Custody

Question 2.1. Capacity to hold issuer reserve deposits

- **Tier 1.** The institution has not evaluated whether its core processor, deposit operations, and FDIC insurance structure can accommodate a payment stablecoin issuer's reserve cash deposits. No conversation has occurred with the institution's correspondent bank or with a placement network (IntraFi, R&T Deposit Solutions, Promontory).
- **Tier 2.** The institution has evaluated capacity, has identified the operational adjustments required to accept reserve deposits (account-titling, sub-accounting, statement cadence, reporting), and has a documented capacity ceiling above which it would need to participate through a placement network.
- **Tier 3.** The institution is enrolled in a reciprocal deposit network (IntraFi ICS or equivalent), the operational adjustments are in place, the chief financial officer has modeled the net interest margin impact of receiving reserve-deposit flows, and the institution has identified at least one stablecoin issuer with which it has had an introductory conversation.

Question 2.2. Treasury management for digital-asset positions

- **Tier 1.** The institution has not addressed how it would custody digital assets, manage the on-chain side of any future activity, or account for digital-asset positions on its general ledger.
- **Tier 2.** The institution has identified a qualified custodian (Anchorage Digital Bank, BitGo Trust, Fidelity Digital Assets) or has researched at least two candidates. The chief financial officer has reviewed the accounting treatment under FASB ASU 2023-08 and the tax treatment under IRS Revenue Ruling 2023-14.
- **Tier 3.** The institution has selected a custody pathway (third-party qualified custodian, partnership with a federally chartered trust bank, or in-house under a state trust authority), the accounting and tax treatment is documented in the institution's accounting policies, and the chief financial officer has run a tabletop scenario covering the lifecycle of a hypothetical digital-asset position.

Question 2.3. Liquidity stress and concentration modeling

- **Tier 1.** Liquidity stress testing does not consider digital-asset-related scenarios (reserve-deposit run, stablecoin issuer failure, fourth-party blockchain network outage).
- **Tier 2.** The institution has added at least one digital-asset scenario to its liquidity stress testing, but the scenario has not been reviewed by the asset-liability committee or presented to the board.
- **Tier 3.** Digital-asset scenarios are integrated into the institution's liquidity stress framework, the asset-liability committee has reviewed at least one full cycle of stress results, the board has received a summary, and the institution's contingency funding plan covers a reserve-deposit redemption stress event.

Dimension 3. Technology and Blockchain Operations

Question 3.1. Core processor and digital-asset capability

- **Tier 1.** The institution has not asked its core processor (Fiserv, Jack Henry, FIS, others) whether the platform supports stablecoin-related deposit operations, on-chain transfer initiation, or reserve-deposit servicing.
- **Tier 2.** The institution has asked the core processor and has received a written response identifying available capabilities, in-development capabilities, and gaps. The response has been logged in the technology roadmap.
- **Tier 3.** The institution's technology roadmap reflects the core processor's stablecoin capability, the chief technology officer has identified the path to fill any gaps (vendor add-ons, middleware, alternative processors), and the institution has tested at least one capability in a sandbox environment.

Question 3.2. On-chain analytics and transaction monitoring

- **Tier 1.** The institution does not have a relationship with an on-chain analytics provider (Chainalysis, TRM Labs, Elliptic) and has not evaluated whether the BSA/AML monitoring stack would need to ingest on-chain alerts.

- **Tier 2.** The institution has evaluated at least two on-chain analytics providers, understands the cost structure, and has identified the integration points with the existing BSA/AML monitoring system.
- **Tier 3.** The institution has either (a) contracted with an on-chain analytics provider, or (b) confirmed that the BSA/AML risk profile does not require direct on-chain monitoring because the institution's role is limited to a layer (reserve-deposit custody, for example) where on-chain monitoring is the vendor's responsibility and is contractually pushed to the bank.

Question 3.3. Cybersecurity readiness for the 36-hour rule

- **Tier 1.** The institution's incident response plan does not specifically address computer-security incidents involving digital-asset activities, vendor cyber breaches affecting reserve deposits or custody, or on-chain incidents (smart-contract exploits, network forks).
- **Tier 2.** The incident response plan has been amended to address digital-asset incidents, the 36-hour notification rule (12 CFR Part 304 Subpart D) is referenced, and the chief information security officer has identified the trigger criteria.
- **Tier 3.** The amended incident response plan has been tested in a tabletop exercise within the past 12 months, the tabletop included at least one digital-asset scenario, lessons learned were documented, and the plan was updated based on the exercise.

Dimension 4. Third-Party and Fourth-Party Risk Management

Question 4.1. Vendor file structure

- **Tier 1.** The institution's third-party risk management file structure does not specifically address digital-asset vendors. The institution would build the file from scratch for the first stablecoin vendor.
- **Tier 2.** The institution has adopted the five-document file structure (board-approved risk appetite memo, completed due diligence record, executed contract and exhibits, ongoing monitoring log, tested termination plan) and has confirmed it applies to digital-asset vendors. A vendor due diligence questionnaire covering digital-asset risk topics is available.
- **Tier 3.** The five-document structure is in production use, at least one digital-asset vendor file has been built (even if the relationship was declined at diligence), and the institution's vendor management committee has reviewed the file.

Question 4.2. Contractual readiness

- **Tier 1.** The institution's standard vendor master services agreement template does not include the provisions specific to digital-asset risk (data ownership on termination, examiner access, fourth-party audit rights, indemnification scope covering on-chain risk, custody segregation, bankruptcy remoteness).
- **Tier 2.** The institution has either drafted or licensed a digital-asset-specific addendum to the master services agreement, but the addendum has not been used in production.

- **Tier 3.** The digital-asset addendum has been used in at least one vendor engagement (even if the engagement was a diligence-stage walkaway), legal counsel has reviewed the addendum against the institution's risk appetite, and the addendum is reviewed annually.

Question 4.3. Fourth-party visibility

- **Tier 1.** The institution does not request or track its digital-asset vendors' fourth-party dependencies (custodians, banking partners, blockchain infrastructure providers, audit firms).
- **Tier 2.** The institution requests a fourth-party inventory at vendor onboarding but does not monitor changes or assess fourth-party concentration risk across the institution's vendor portfolio.
- **Tier 3.** The institution maintains a current fourth-party inventory for every digital-asset vendor, monitors changes through ongoing vendor monitoring, and reviews fourth-party concentration risk at the vendor management committee at least annually.

Dimension 5. Customer-Facing and Frontline

Question 5.1. Frontline staff training

- **Tier 1.** Frontline staff (tellers, customer service, branch managers, commercial lenders) have received no formal training on stablecoins, on-chain activity, or the regulatory framework. Frontline conversations with customers asking about stablecoins are unscripted.
- **Tier 2.** Frontline staff have received at least one training session covering the basics: what a stablecoin is, what the institution's current position is, and where to escalate customer questions. Training has not been refreshed in the current cycle.
- **Tier 3.** Frontline training is part of the institution's annual training program, the institution has produced a one-page customer-facing fact sheet that staff can hand to customers, escalation paths are documented, and the chief retail officer (or equivalent) can confirm staff readiness on a spot check.

Question 5.2. Customer-facing position and disclosures

- **Tier 1.** The institution does not have a public-facing position on stablecoins. Customers asking about the topic receive ad-hoc responses that vary by branch and by staff member.
- **Tier 2.** The institution has drafted a customer-facing position statement covering whether the institution offers stablecoin-related products, what the customer should expect, and where to find more information. The statement has been reviewed by compliance but not approved by the board or published.
- **Tier 3.** The customer-facing position statement has been board-approved, published on the institution's website, and integrated into account-opening disclosures where relevant. The chief marketing officer or chief retail officer has reviewed the statement against UDAAP standards and the consumer-protection provisions of CLARITY Act § 404.

Question 5.3. Reputation and regional or community bank franchise

- **Tier 1.** The institution has not considered how stablecoin activities (or the deliberate decision not to engage) would be communicated to the institution's community, board, and shareholder base. The conversation has not started.
- **Tier 2.** The institution has started the conversation internally (executive team and board), has identified the likely community concerns and the likely community opportunities, but has not produced any external communications.
- **Tier 3.** The institution has a communications posture appropriate to its market: a board-approved position, an external communications plan if engaged, a community-stakeholder engagement strategy, and a defensible answer to the question a state legislator or community newspaper might ask.

Scoring

Step 1. Tally tier counts.

Count the number of questions scored at each tier. Total questions: 15.

- Tier 3 (Operating): ___ of 15
- Tier 2 (Foundational): ___ of 15
- Tier 1 (Not Ready): ___ of 15

Step 2. Apply weights.

Multiply each count by the tier weight, sum the products.

- Tier 3 count × 3 = ___
- Tier 2 count × 2 = ___
- Tier 1 count × 1 = ___
- **Total readiness score: ___ out of 45**

Step 3. Interpret the score.

Score Range	Readiness Profile	Recommended Next Step
37 to 45	Examination-ready	Move to active vendor engagement. The institution can defend its current state to a board, a regulator, and a community stakeholder.
28 to 36	Foundational	Identify the specific Tier 1 and Tier 2 gaps that block movement to the next stage. Build a 90-day work plan. The institution is ready to engage in vendor diligence but is not yet ready to launch a customer-facing product.
19 to 27	Preparatory	Foundational governance and policy work is still required. Engaging a vendor today would create a documented gap in the third-party risk-management file. Spend the next two quarters closing governance and policy gaps before vendor diligence.
15 to 18	Pre-readiness	The institution is at baseline. The board has not yet engaged with the topic at a working level. Use the Hickory framework and the broader regulatory record (OCC Interpretive Letters, GENIUS Act, CLARITY Act) to bring the board to a Tier 2 position on governance and strategy before any vendor conversation begins.

Step 4. Identify the three highest-priority gaps.

List the three lowest-tier scores. These are the next-quarter work items. A gap in Dimension 1 (Governance and Strategy) almost always blocks progress in the other four dimensions, so weight those gaps highest.

1.
2.
3.

Step 5. Calendar the refresh.

Score this assessment quarterly through the build-out phase, then annually once the institution is at a Tier 3 average. Track the trend in the institution's enterprise risk management dashboard.

Companion document

This self-assessment is paired with the **Stablecoin Vendor Due Diligence Request List** (50 items, separate handout). The self-assessment measures the institution's internal readiness; the vendor DDQ measures any prospective vendor's external readiness. Both populate the third-party risk-management file structure every examiner expects.

Citations

[1] GENIUS Act, Pub. L. No. 119-27, July 18, 2025.

[2] CLARITY Act, draft, § 404 (yield prohibition) and Title V (Bank Activities in Digital Assets), Senate Banking Committee, May 2026.

[3] OCC Interpretive Letter 1172, January 4, 2021 (stablecoin reserve holding).

[4] OCC Interpretive Letter 1174, January 4, 2021 (validator node operations).

[5] OCC Interpretive Letter 1183, November 18, 2021.

[6] OCC Interpretive Letter 1184, March 7, 2025 (removal of supervisory non-objection requirement).

[7] FDIC, FIL-7-2025, "Withdrawal of FIL-16-2022," March 28, 2025.

[8] Federal Reserve Board, withdrawal of SR 22-6, April 24, 2025.

[9] FFIEC member agencies, Interagency Guidance on Third-Party Relationships: Risk Management, June 6, 2023.

[10] FDIC, OCC, Federal Reserve, Computer-Security Incident Notification Rule, 12 CFR Part 304 Subpart D and parallel agency rules, effective May 1, 2022.

[11] FASB Accounting Standards Update (ASU) 2023-08, December 2023.

[12] Internal Revenue Service, Revenue Ruling 2023-14, August 1, 2023.

[13] FinCEN, Bank Secrecy Act regulations, 31 CFR Chapter X.
