

DIGITALTRADE4.EU, RIHO VEDLER

Proposal and Comment Information

Title: Application Procedures for Board-Supervised Insured Depository Institutions Seeking Approval for a Subsidiary to Issue Payment Stablecoins, R-1900

Comment ID: FR-2026-0034-01-C09

Submitter Information

Organization Name: DigitalTrade4.EU

Organization Type: Foreign

Name: Riho Vedler

Submitted Date: 10/08/2026

DigitalTrade4.EU submits this feedback on Federal Reserve Docket No. R-1900 to highlight the importance of external dependency governance, interoperability, and operational resilience in payment stablecoin applications.

As payment systems become increasingly connected with digital trade, logistics, financial infrastructure, and external verification services, payment and settlement decisions may depend on information originating outside the direct control of the stablecoin issuer. These dependencies can introduce risks related to data integrity, authorization, accountability, operational continuity, and the reliability of automated financial processes.

Drawing on its research into Verified Trade Events (VTE) and digital trade interoperability, DigitalTrade4.EU emphasizes the importance of distinguishing underlying commercial events from their supporting evidence, verification or attestation, and the financial instructions that follow. This distinction helps clarify where responsibility lies, how external information influences financial decisions, and which controls must remain under the authority of the payment stablecoin issuer.

The central recommendation is to make material external dependencies more transparent within the existing regulatory application framework. Rather than introducing new reporting structures or additional regulatory obligations, applicants should be encouraged to explain how they identify, assess, govern, monitor, and respond to dependencies that could materially affect payment or redemption outcomes.

Particular attention should be given to clear organizational accountability, effective intervention and recovery capabilities, independent oversight, and the ability to adapt to evolving technical standards, cybersecurity threats, and operational risks. These considerations are especially relevant where multiple organizations share infrastructure, data services, or verification responsibilities.

DigitalTrade4.EU also emphasizes that dependency governance should be an ongoing process rather than a one-time application exercise. Changes in technology, external service providers, standards, and risk conditions should be subject to appropriate internal review, escalation, and corrective action, with regulatory information updated when materially necessary.

Importantly, the proposed approach preserves a clear boundary between financial supervision and the verification of underlying commercial activities. The Federal Reserve should be able to assess whether a stablecoin issuer maintains effective control over its financial operations without being expected to determine the substantive validity of trade documents, logistics records, or commercial events.

The objective of this feedback is to support a proportionate, technology-neutral, and future-oriented regulatory framework that strengthens accountability, transparency, and operational resilience while enabling responsible innovation and interoperability between payment stablecoins and the wider digital economy.

The accompanying technical document provides the detailed regulatory analysis, proposed governance mechanisms, illustrative control structures, and practical implementation recommendations supporting these observations.

External Dependency Governance and Interoperability in Payment Stablecoin Applications

DigitalTrade4.EU

Contact: Riho Vedler | secretariat@digitaltrade4.eu | October 2026 | v5

Abstract. This technical note proposes a proportionate, technology-neutral approach to identifying and governing material external dependencies in applications under Federal Reserve Docket R-1900. Drawing on the Verified Trade Events (VTE) perspective, it distinguishes commercial events, supporting evidence, verification or attestation, and resulting payment or settlement instructions. The central supervisory question is whether the applicant and proposed Board-supervised payment stablecoin issuer (PPSI) can demonstrate effective control, accountability, intervention capability, reconciliation, and operational resilience where external data or attestations may affect payment or redemption outcomes.

The proposed approach integrates statutory-factor mapping, risk-based dependency assessment, standardized disclosure fields embedded in existing application materials, entity-specific accountability in consortium arrangements, issuer-controlled intervention mechanisms, and a Question 17 delta schedule for multiple payment stablecoins. It also addresses operational-loss pathways relevant to R-1899 and governance arrangements for independent challenge, escalation, information sharing, periodic review, and structured issue remediation. Material changes are assessed against the continuing sufficiency of the application record under proposed § 247.30(c)(2).

The objective is to make material dependencies transparent, reviewable, and subject to durable PPSI governance without creating a separate filing requirement, prescribing technical standards, introducing new prudential criteria, or requiring the Federal Reserve to validate underlying commercial events, trade documents, or logistics evidence.

KEY WORDS. payment stablecoins; verified trade events; interoperability; application governance; operational resilience.

1. Introduction

Federal Reserve Docket No. R-1900 proposes a tailored application process for an insured State member bank seeking approval for a subsidiary to issue payment stablecoins. The proposal states that the application must contain enough information for the Board to evaluate the statutory factors in section 5(c) of the GENIUS Act and whether the proposed activities would be unsafe or unsound. It requires, among other things, a business plan, financial information, relevant policies and agreements, specified capital-structure information, and certifications. The business plan is expected to describe governance, material third-party relationships, and the identities, roles and responsibilities of entities involved in related activities; the supporting policies are expected to cover transaction processing, recordkeeping and reconciliation.¹

Those information requirements create a direct point of contact with DigitalTrade4EU research on Verified Trade Events (VTE) and trade-finance interoperability. A payment or financing outcome may depend on a fact generated outside the payment system: delivery, control of an electronic bill of lading, invoice approval, inspection, warehouse status, customs release, acceptance, or another contractual milestone. The PPSI may not ingest the underlying commercial record. It may instead receive an assertion, attestation, reference or status message. The application-review question is therefore whether the PPSI understands and controls the dependency through which that external information can influence a financial action.

The VTE model separates four functions that are often collapsed in architecture descriptions: the commercial event; evidence representing the event; verification or attestation that gives the evidence a defined trust status; and the payment or settlement instruction that follows. This separation makes it possible to test identity and authority, provenance, correction and revocation, sequencing, exception handling, reconciliation and operational fallback without prescribing a particular ledger, oracle, messaging standard or trade-document platform.

Supervisory boundary—The Board need not and should not become an adjudicator of whether goods were delivered, whether an electronic bill of lading is commercially valid, or whether a logistics record is substantively correct. The relevant R-1900 inquiry is whether the applicant and proposed PPSI have identified a material dependency, assigned accountability, established reasonable controls over the source and authority of inputs, retained issuer-level compliance and intervention capability, and can reconcile and recover when the dependency fails. Under this approach, VTE is a way to describe the PPSI control perimeter, not a request for the Federal Reserve to supervise trade-document content.¹

This feedback therefore keeps the core recommendation narrow. Rather than ask the Board to administer a separate optional annex, R-1900 could encourage a small set of standardized external-dependency fields within the business plan, transaction-processing policies, third-party materials, or other information already required by the proposal. Applicants could cross-reference existing enterprise documentation where it contains the same facts. The additional governance proposal in this feedback concerns how the PPSI assigns internal accountability and keeps those dependency facts current over time; it does not ask the Board to supervise the underlying trade standard, logistics evidence, or commercial event.

2. Regulatory Mapping and the Limits of the Review

R-1900 already provides the legal and procedural hooks needed to consider material external dependencies. Section 5(c)(1) requires the Board to evaluate the proposed PPSI's ability, based on financial condition and resources, to meet section 4 requirements; the proposal identifies capital, liquidity and risk management, BSA and sanctions compliance, permissible-activity limitations, and technological capability to comply with lawful orders among those requirements. Section 5(c)(3) concerns the competence, experience and integrity of specified management and owners, including their ability to fulfill commitments and conditions. Section 5(c)(4) concerns the redemption policy. Section 5(c)(2), by contrast, addresses specified felony convictions and generally does not call for a separate VTE-specific information layer.¹

The mapping should be selective. Most VTE-related information supports section 5(c)(1) because it shows how the PPSI will control transaction processing, third-party dependencies, reconciliation and compliance. It may support section 5(c)(3) where the issue is whether management has identified and can govern a critical dependency. Section 5(c)(4) is relevant only where the external dependency affects redemption itself. None of these factors requires the

Board to validate the underlying trade fact; the evidence should show the PPSI's control environment and decision path.

Table 1. Regulatory mapping of VTE information to R-1900 review.

VTE / dependency element	R-1900 application evidence	Statutory factor	Review purpose
Commercial event / condition	Business model; products, services and activities; transaction-processing policy.	§5(c)(1); §5(c)(4) only if redemption is affected.	Which external fact can change a financial outcome; not whether the fact is commercially correct.
Evidence and source	Material third-party relationships; identities, roles and responsibilities; recordkeeping.	Primarily §5(c)(1).	Provenance, source governance and whether the PPSI receives source data, a reference or only an attestation.
Verification / attestation	Third-party agreements; governance; transaction processing; risk management.	§5(c)(1); §5(c)(3) indirectly through oversight capability.	Who is authorized to verify, how that authority is controlled, and what happens if verification fails.
Identity and authority	Governance; access and authorization controls; BSA/sanctions controls where applicable.	Primarily §5(c)(1); potentially §5(c)(3).	Whether the PPSI can attribute a message and determine authority to make the relevant assertion.
Settlement instruction / trigger	Transaction processing; roles and responsibilities; lawful-order capability.	§5(c)(1).	How an external status becomes a financial action and where issuer-level controls remain effective.
Reconciliation / audit reference	Recordkeeping, reconciliation and transaction-processing policies.	§5(c)(1).	Whether the PPSI can reconstruct why a transaction occurred without the Board validating the trade record.
Redemption dependency	Redemption policy, customer terms, processing and third-party arrangements.	§5(c)(4), plus §5(c)(1).	Relevant only when external data or a third party can delay, condition or alter redemption.
Internal governance / periodic review	Governance; risk management; material third-party oversight; change control; application maintenance.	Primarily §5(c)(1); §5(c)(3) where management capability is relevant.	Who owns and challenges the dependency, how standards/cyber changes are reviewed, how recurring issues are learned from, and when application information must be updated.

Question 9: no new standalone factor is necessary—The external-dependency issue can be handled as cross-cutting information supporting the existing statutory factors and safety-and-soundness analysis. Creating a separate factor risks duplicating section 5(c)(1) and the proposal's existing requests for material third-party, governance, transaction-processing and

recordkeeping information. A clearer and less burdensome approach is to specify when those existing categories should include dependency information.

Question 10: control evidence, not trade-document adjudication—Where a material external dependency exists, useful supporting material could include a data-flow diagram, identity and authorization controls, change-control and exception procedures, reconciliation logic, continuity arrangements, and a concise description of the external decision point. The purpose is to identify control points and accountability. The Board should not need the underlying commercial record merely because it is the source of an external status unless that record is independently necessary to evaluate a statutory factor.

3. Materiality, Risk Triage and the R-1899 Prudential Cross-Reference

A dependency should be treated as material for application purposes when its failure, corruption, delay, misidentification or unauthorized use could materially change a payment or redemption outcome, defeat a required control, prevent reliable reconciliation, or create a significant operational-loss pathway. This is consistent with R-1900's completeness standard: the relevant question is whether information about the dependency is necessary for the Board to evaluate the statutory factors, not whether the underlying technology is novel.¹

The following three-level tier can help determine the amount of information that should accompany an application. It is intentionally qualitative and should not be interpreted as a capital bucket. R-1900 requires applicants to demonstrate the ability to comply with applicable capital rules and, before those rules become effective, to support the proposed volume and type of business with sufficient initial and longer-term capital. The parallel R-1899 proposal would separately calculate operational-risk capital using issuance and non-reserve revenue measures, adjusted by a loss scalar based on realized operational losses. External dependencies are therefore relevant to capital planning when they create credible operational-loss scenarios, but the R-1900 application should not mechanically translate a dependency tier into a capital percentage.¹²

Table 2. Illustrative external-dependency disclosure tier (not a regulatory rating or capital category).

Tier	Indicative characteristics	Application evidence	Illustrative case
Low	Failure does not directly change amount, recipient, redemption right or final settlement; a validated alternative source or manual process is available.	Identify the dependency and owner; cross-reference ordinary vendor/change documentation.	Non-critical enrichment data or a redundant status feed.
Medium	Failure can delay or hold a transaction, require manual intervention, or impair reconciliation, but exposure is bounded and a tested fallback exists.	Describe authority model, fallback, reconciliation and escalation; cross-reference relevant third-party controls.	External event used to release a payment subject to manual dual control if unavailable.
High	Dependency can directly trigger, block or misdirect settlement/redemption; compromise can defeat reconciliation or lawful-order controls; or a third party has critical key, mint/redeem or unique attestation authority.	Provide the standardized dependency fields, data-flow, governance, intervention controls, continuity testing and change triggers.	Unique attester whose signed event directly activates a settlement instruction.

Technology-neutral example: Verified Delivery Event—Assume a trade-finance arrangement releases a payment after delivery. A logistics or trade-document system records delivery; an authorized verifier issues a delivery attestation containing a stable event identifier; the PPSI or connected payment service validates the verifier's credential and the event status; and the resulting instruction releases payment. The application need not require the Fed to choose the trade-document platform or determine whether delivery occurred. It should show the control chain:

- **Event:** the contractual condition the PPSI is configured to recognize, without asking the Board to adjudicate the underlying commercial fact.
- **Evidence reference:** the record or source identifier used by the PPSI and how provenance is maintained.
- **Verification:** the verifier, its authority, credential status, and rules for correction or revocation.
- **Settlement trigger:** the exact machine or human decision condition that converts the verified status into a payment instruction.
- Exceptions: action for conflicting, stale, duplicated, unavailable, compromised or disputed evidence.
- **Audit link:** a stable identifier connecting the payment record to the event reference, verifier decision and exception history.

R-1899 cross-reference: identify loss pathways, do not import the capital formula into R-1900—R-1899 proposes an operational-risk capital requirement equal to a baseline requirement multiplied by a loss scalar based on historical operational losses. It also proposes collection and classification of operational loss events, including categories such as external fraud, business disruption and system failures, and execution, delivery and process management. A compromised attester, false external status, or failed dependency could generate losses that ultimately fall within one of those categories depending on the facts. For R-1900 purposes, the useful application-stage disclosure is therefore the plausible loss pathway, control owner,

detection point and recovery process. The Board need not assign an R-1899 loss category or capital charge at the application stage solely because a VTE dependency exists.²

This cross-reference creates a practical benefit: stable event identifiers, verifier-status records, occurrence/discovery timestamps, override history and reconciliation links can later support operational-loss root-cause analysis if a covered loss occurs. That is a data-governance benefit, not a recommendation to change the R-1899 calibration.²

4. Lawful-Order Capability, Intervention Points, Recordkeeping and Reconciliation

Lawful-order capability—R-1900 treats the proposed PPSI's ability to meet section 4 requirements as a statutory factor, and the Board's parallel GENIUS Act proposal identifies technological capability to comply, and actual compliance, with the terms of lawful orders as a statutory requirement. An application involving externally triggered payments should therefore explain how an external attestation interacts with issuer-level compliance controls. The disclosure should identify the processing stages at which the PPSI can suspend or quarantine a pending trigger, disable or reject a compromised credential, prevent automatic re-processing, and document the reason and authority for intervention.¹²

Circuit breaker for a compromised attester—A practical control pattern is an issuer-controlled circuit breaker. If an attester or credential is suspected of compromise, the PPSI should be able, where technically and legally available, to move that attester into a quarantined state; stop new automated actions that depend on it; route affected pending items to an exception queue; identify transactions processed since the last trusted checkpoint; reconcile or investigate those items; and restore automated processing only under defined authorization. The application should identify who has authority to invoke and release the circuit breaker, how dual control or equivalent safeguards apply, and how the action is logged. This describes an operational control, not a requirement that any particular blockchain implement a specific pause function.

Pre-finality and post-finality boundaries—The application should identify the latest issuer-controlled point at which a pending external trigger can be stopped before the payment becomes final under the relevant system rules. Once a transfer is legally or technically final, the PPSI should describe the controls that remain lawfully available rather than imply a general power to reverse final transactions. The lawful-order requirement concerns capability to comply with an order; the particular response will depend on the order, applicable law, contract, network design and transaction state.²

Recordkeeping and audit traceability—R-1900 expressly requests policies and procedures covering recordkeeping, reconciliation, transaction processing and BSA compliance. For a material external dependency, a reconstructable audit chain should normally preserve the transaction identifier, external event or evidence reference, verifier identity and authority state, decision status and timestamp, exception or override history, and the link to the resulting payment instruction. This allows reconciliation without requiring the PPSI to copy every underlying commercial document into its own ledger.¹

BSA retention: apply the rule to the records it actually covers—FinCEN's general BSA record-retention rule provides that records required to be retained under the BSA regulations are generally retained for five years. That does not mean every VTE event record automatically becomes a five-year BSA record. The application should instead classify which dependency records are required for BSA/AML or other regulatory purposes, identify the applicable retention period, and ensure that those records remain reasonably accessible. Other event and

interoperability records can be retained according to the PPSI's separate legal, operational and contractual requirements.³

5. Consortium Structures: Shared Infrastructure Without Diluted Accountability

Questions 1-5, 12 and 19 make the control analysis central to consortium and non-wholly-owned structures. R-1900 incorporates the BHC Act control framework through the FDI Act definition of subsidiary and asks how the control requirement affects consortium models. The proposal also states that the Board may accept and process a single application on behalf of all insured State member banks in a consortium if the consortium could be considered a subsidiary of each. That procedural flexibility should not obscure entity-specific responsibility.¹

Operational dependency versus controlling influence under BHC Act §2(a)(2)—A technology provider, attestation service or shared platform can be operationally critical without thereby controlling the PPSI. Conversely, contractual or governance rights may become relevant to the control analysis when they confer meaningful influence over management or policy. For application purposes, the useful disclosure is a rights map: who can appoint or remove decision-makers; approve budgets or business plans; change mint/redeem or key-management permissions; admit participants; approve a critical verifier; alter transaction or settlement rules; or veto material changes. This avoids treating technical dependence itself as a legal conclusion on control.¹

A shared technical description is evidentiary convenience, not shared legal responsibility—If consortium members use common infrastructure, a shared technical description can reduce duplicative drafting and version drift. It should not operate as a substitute for each applicant's own application responsibility or for the proposed PPSI's own ability to satisfy the GENIUS Act requirements. Each applicant relying on common material should expressly identify the portions it adopts, certify or otherwise stand behind the facts it submits as part of its filing, and provide its own ownership, governance, financial-support, risk-appetite and responsibility information. The common document should identify a version owner and change-control process so that every relying applicant can determine when its own filing record needs to be supplemented.¹

Capital and loss responsibility should follow the legal structure—R-1900 asks whether the proposed PPSI can meet applicable capital requirements and requests information about funding, financial guarantees, intercompany agreements and consortium-related financial support. R-1899 separately proposes capital requirements for the Board-supervised PPSI. The application should therefore identify which legal entity bears a service obligation, guarantee, indemnity, remediation cost or other loss exposure arising from a shared dependency. It should not assume that a common technology layer creates common liability or that an operational dependency reallocates regulatory capital among banks.¹²

Table 3. Shared infrastructure, entity-specific accountability and loss pathways.

Shared dependency	Common governance	Applicant / PPSI accountability	Financial / loss-path disclosure
Shared attestation service	PPSI or consortium body that approves provider and verification policy	Each relying applicant identifies its adoption, oversight role and escalation path.	Identify contractual obligations, indemnities, fallback and entity that bears remediation cost.
Shared identity / onboarding framework	Entity with rule-setting and credential-governance authority	Each applicant identifies its own participant-eligibility and exception responsibilities.	Show whether failure creates loss, compliance or reporting obligations for the PPSI or a member bank.
Shared transaction / smart-contract layer	Entity controlling code deployment, key management and emergency controls	Each applicant identifies rights, vetoes and issuer-level intervention capability.	Identify support arrangements and who bears code-remediation, incident-response or customer-loss costs.
Shared reconciliation service	Entity responsible for ledger-to-record matching and exception resolution	Each applicant identifies who receives, reviews and resolves its own breaks.	Identify responsibility for corrections, record availability and any resulting operational loss.

Questions 4 and 5: filing architecture—A workable consortium filing can use common factual material for shared infrastructure, but the application architecture should preserve a clear legal chain from each applicant to the PPSI and to any common component. Where the Board accepts a single consortium application, the filing can identify common sections once and use applicant-specific schedules for ownership, governance, financial commitments, responsibilities and certifications. The objective is one source of technical truth with no ambiguity about which legal entity is responsible for what.¹

6. Completeness and the Material-Change Test under Proposed § 247.30(c)(2)

R-1900 provides that an application deemed substantially complete may later be treated as no longer substantially complete if a material change in circumstances means that the information received as of the submission date is no longer sufficient for the Board to evaluate all statutory factors. The proposal gives deterioration in the applicant's financial condition, a material alteration of the PPSI business plan, and changes in ownership structure as examples. If supplementary information restores the Board's ability to decide the application, the proposal would assign a new submission date and restart the 120-day clock.¹

For technical and interoperability changes, the same statutory test should apply. The relevant question is not whether an API, network or provider changed, but whether the change makes the existing application record insufficient to evaluate a statutory factor. Table 4 is therefore an indicative screening tool, not a legal determination. Applicants should update the record when needed; whether a change is sufficiently material to reset completeness remains for the Board under the proposed rule.

Table 4. Indicative material-change screening under proposed § 247.30(c)(2).

Change type	Indicative screening	Reason	Recommended application action
Routine API patch, syntax revision or infrastructure maintenance with no change in authority, data semantics, fallback or transaction outcome	Usually low	Existing record remains sufficient if control environment and statutory-factor analysis are unchanged.	Maintain internal change log; supplement only if previously submitted facts become inaccurate or incomplete.
Schema or validation change that alters event meaning, accepted evidence or exception handling	Potentially material	Can change what fact triggers payment and how errors are detected.	Update standardized dependency fields and relevant procedures; assess whether the statutory-factor record remains sufficient.
Replacement of a critical attestation provider or credential authority	Potentially / likely material for high-risk dependencies	Changes third-party relationship, authority model, resilience and possibly management oversight.	Promptly supplement relevant facts; include due diligence, migration, fallback and reconciliation changes.
Change to settlement-trigger logic, mint/redeem authority or key-control model	Likely material where outcome or control changes	Can directly change transaction outcome, lawful-order capability or control environment.	Supplement application and discuss treatment before implementation during pendency where appropriate.
Change in ownership, principal governance rights or consortium decision rights	Likely material; ownership change is an express example	May affect control analysis and management/governance statutory factors.	Supplement application; expect the Board to reassess completeness as appropriate.
Move to a different network with equivalent governance and control architecture	Fact-specific	Network change is not necessarily material if the existing statutory-factor record remains sufficient.	Provide a focused delta of control, resilience, keys, processing and reconciliation.
New stablecoin using the same control environment	Fact-specific	Shared controls can be cross-referenced, but token-specific differences may still affect review.	Provide the Question 17 Delta Schedule described below; follow Board conditions and filing expectations.

Question 6: clarification would reduce avoidable clock resets—The Board could clarify that technical changes should be assessed by their effect on the sufficiency of the statutory-factor record, with non-exclusive examples for critical third-party, authority, settlement-logic and governance changes. Such clarification would give applicants an incentive to maintain current dependency information without implying that every software release restarts the application.

7. Question 17: A Standardized Delta Schedule for Multiple Payment Stablecoins

Question 17 asks how the Board should review applications from entities proposing to issue more than one payment stablecoin and whether a new application should be required for each. A standardized delta schedule can separate a common control baseline from token-specific differences. It would not decide whether a new application is legally required; it would give the Board a concise basis for determining whether previously submitted information remains sufficient for the statutory factors and whether additional application material is necessary.¹

Table 5. Illustrative Question 17 Delta Schedule.

Dimension	Common baseline that may be cross-referenced	Token-specific delta	Review significance
Issuer / legal entity and governance	Same PPSI, board and core governance framework.	Different issuing entity, ownership, decision rights or financial support.	Potentially affects control, §5(c)(3), capital/support and filing scope.
Network and smart-contract architecture	Same approved code governance and key-control framework.	Different blockchain, contract model, bridge, key custody or upgrade rights.	Can change operational resilience, third-party reliance and lawful-order capability.
Mint / burn / redemption flow	Same authorities, customer rights and processing controls.	Different mint/burn permissions, redemption channel, timing or intermediaries.	May affect §5(c)(1), §5(c)(4), transaction processing and compliance.
Reserve / custody model	Same reserve categories, custody structure and control framework.	Different custodian, tokenized reserve arrangement or asset-management process.	May alter prudential evidence and third-party dependencies.
Distribution / customer / jurisdiction	Same channels and compliance perimeter.	Different distributors, user segment, jurisdictional exposure or access model.	May change BSA/sanctions, customer-agreement and operational controls.
External event / attestation dependencies	No new material dependency; same providers and rules.	New oracle, attester, trade-event trigger, credential authority or data standard.	Requires dependency review, override controls and materiality assessment.
Lawful-order controls	Same issuer intervention and compliance capabilities.	Different technical ability to restrict, quarantine, freeze or otherwise comply with lawful orders.	Directly relevant to section 4 capability under §5(c)(1).
Reconciliation / recordkeeping	Same identifiers, audit path and exception workflow.	Different ledger-to-record mapping, evidence linkage or exception process.	May alter ability to reconstruct transactions and manage breaks.

Operational-loss profile / continuity	Same failure modes and tested recovery design.	New critical provider, unique failure mode, concentration or recovery dependency.	Relevant to safety and soundness and R-1899 loss-pathway analysis.
--	--	---	--

Burden principle—The applicant should not have to reproduce unchanged enterprise controls for every token. Conversely, a label such as “same issuer” or “same platform” should not substitute for disclosure of a materially different network, redemption flow, attestation model or compliance capability. A delta schedule provides the middle path: reuse the common baseline, disclose only what changes, and let the Board determine what additional filing treatment is needed.

8. Internal Governance, Continuous Review and Issue Learning

Internal governance as application evidence—A material external dependency is not adequately described by naming a provider, interface or standard. The application should also show how the PPSI remains organizationally accountable for that dependency. Useful information includes the accountable business or executive owner, the technical or control owner, decision rights over provider and rule changes, override authority, escalation paths, independent risk or compliance challenge, continuity responsibility, and the function that determines whether a change may require supplementation of the R-1900 application. This information supports review of the PPSI control environment and management capability; it does not transfer responsibility for the substantive correctness of an external commercial event to the PPSI or to the Board.

Role boundaries and segregation of duties—The governance description should distinguish the authority to attest an external event from the authority to alter payment logic, change credentials, release a quarantined dependency, or override a control. An attester may be permitted to make a defined assertion without being able to alter the PPSI's settlement logic. A technology administrator may maintain an interface without unilateral authority to disable compliance controls. Where a critical action can change payment, redemption, key control or lawful-order capability, the application should identify the PPSI-level approval and challenge mechanisms that keep the decision within the issuer's control perimeter.

Table 6. Illustrative internal-governance and review responsibilities for material dependencies.

Governance function	Applicant / PPSI description	Evidence or escalation	R-1900 relevance
Accountable owner	Named function or senior owner accountable for the dependency and its risk acceptance.	Mandate, responsibility map, management reporting line.	Shows entity-level accountability and management control.
Control / technical owner	Function responsible for identity, authorization, interface integrity, validation rules, reconciliation and fallback.	Control inventory, testing evidence, service and change records.	Supports transaction-processing, recordkeeping and third-party review.

Override authority	Who may quarantine a provider or credential, stop automated processing, approve fallback, and authorize controlled reactivation.	Dual control or equivalent safeguard; decision log; incident escalation.	Connects compromised-attester controls to issuer-level intervention capability.
Independent challenge	Risk, compliance, information-security or internal-audit function that can challenge the operational owner. For example, a Technology Risk Function may independently challenge dependency-owner testing and settlement-trigger logic.	Periodic review, findings, remediation tracking and closure evidence.	Demonstrates that critical dependency decisions are not self-approved by the operating function alone.
Standards and cyber review owner	Function responsible for monitoring relevant standards, deprecations, vulnerabilities, threat intelligence and interoperability changes.	Standards watch, cyber review, compatibility tests and change assessments.	Keeps application facts and controls aligned with a changing technical environment.
Issue / guidance owner	Function that maintains recurring-issue mapping and converts lessons learned into updated controls or internal guidance.	Issue register, root-cause record, advisory or implementation note.	Shows a durable feedback loop rather than one-time application documentation.
Material-change assessment	Function responsible for deciding whether a change makes previously submitted information insufficient for a statutory factor.	Documented screening under proposed § 247.30(c)(2); escalation to legal/compliance and application owner.	Links ordinary change governance to the R-1900 completeness test.
Information sharing / management reporting	Defined routing of dependency information upward to management, horizontally across affected control and operating functions, and externally where regulatory reporting or application supplementation is required.	Escalation thresholds; incident or standards-change notice; governance minutes; supervisory notification or application-update decision where applicable.	Shows that material issues and changes reach the appropriate decision level and are not confined to technical operations.

Illustrative governance flow—A concise application-facing escalation path could be expressed as: **Dependency Owner -> Independent Challenge Function -> Technology/Operational Risk Governance Committee -> Senior Management**, with board-level escalation where existing risk or incident thresholds are met. For example, a Technology Risk Function could independently challenge dependency-owner testing and settlement-trigger logic before a high-risk change is approved, with unresolved findings escalated to the relevant governance committee. This is an illustrative accountability flow, not a proposed mandatory organizational chart.

A time dimension is essential—External dependencies do not remain static after an application is prepared. Standards are amended or deprecated, new standards emerge, credential

and identity schemes evolve, threat techniques change, provider control environments change, and repeated implementation problems can reveal weaknesses not visible during initial design. A strong governance model therefore combines continuous monitoring, event-driven reassessment and periodic critical review. The Board would not need to prescribe or administer the technical review itself; the application would show that the PPSI has a credible process for maintaining its own control environment.

Illustrative risk-based review cadence—The precise frequency should depend on materiality, complexity and change velocity rather than become a fixed Federal Reserve technical-refresh rule. As an example of internal governance, cybersecurity and control effectiveness for high-risk dependencies could be critically reviewed at least annually; standards, schemas, identity and interoperability baselines could be reviewed on a 12-to-24-month cycle; and the full dependency-governance framework could be reassessed every two to three years. An end-to-end 24-to-36-month review could explicitly challenge dependency controls, authority models, fallback logic, override capability, reconciliation design and cybersecurity posture rather than merely confirm that documentation remains current. Any significant incident, vulnerability, provider compromise, standard deprecation, semantic change, control failure or repeated reconciliation problem should trigger an event-driven review without waiting for the periodic cycle. These intervals are illustrative governance practices, not proposed R-1900 filing deadlines.

Standards and cybersecurity watch—The review process should identify standards that are new, materially amended, deprecated or no longer interoperable with the PPSI's approved design; determine affected interfaces and dependencies; test backward compatibility and migration paths; and assign an implementation decision and owner. Cybersecurity review should examine the dependency-specific attack surface, identity and credential compromise, key and authorization controls, third-party incidents, anomalous event patterns, recovery capability, and whether a control assumed in the application remains effective. The point is not to have the Board select a standard, but to show that the PPSI knows when a technical change alters its risk or control assumptions.

Issue and Standards Review Register—Recurring implementation problems should be mapped in a structured register rather than handled only as isolated tickets. At minimum, useful issue categories can include dependency failures or degraded service, override or circuit-breaker events, reconciliation breaks, and attester or credential compromise; organizations may add standards or semantic conflicts, repeated fallback use, access-control failures and other recurring patterns relevant to their architecture. A useful record can identify the affected dependency or standard, issue type and source, operational and settlement/reconciliation impact, cybersecurity relevance, root cause, interim workaround, permanent remediation, accountable owner, target date, guidance or control that must be updated, and whether the issue triggers an R-1900 material-change assessment. Aggregating near misses and repeated low-severity failures can reveal a control weakness before it becomes a major incident.

Guidance maintenance and ongoing information sharing—Findings should feed back into controlled internal guidance, runbooks, implementation notes, provider requirements and test cases. Information should move through defined channels according to purpose and sensitivity. Upward reporting should surface high-risk incidents, unresolved control gaps, repeated reconciliation breaks, material override events, significant standards or cyber changes, and material-change decisions to the relevant management or board-level forum under the PPSI's existing escalation thresholds. Horizontal sharing should provide affected operational, technology, risk, compliance, legal and, where applicable, consortium or provider functions with the implementation details and lessons needed to maintain consistent controls. Supervisory

communication should remain limited to information required by applicable reporting obligations or needed to supplement the R-1900 application when previously submitted information is no longer sufficient. Information sharing should remain role-based and respect confidentiality, security and customer-data restrictions.

Prior DigitalTrade4.EU governance work provides a useful design precedent, not a legal transplant—The 2025 EUTIR research combined ongoing incident-information exchange and annual reporting with a three-year framework review, a 24-month technical-specification review cycle, and explicit suspension/root-cause/re-activation logic for cybersecurity or system failures. The transferable principle for R-1900 is the feedback loop: monitor, identify issues, escalate, remediate, update guidance and periodically challenge the baseline. The EU-specific supervisory bodies, certification structure and fixed cycles should not be imported into the Federal Reserve application framework as such.⁶

9. Filing Format and Implementation Guidance

Question 8: standardized fields inside the existing application are preferable to a new optional annex—A narrative letter remains useful for explaining the business model and legal context. For recurring technical facts, however, the Board could identify a concise set of standardized fields that applicants include within the business plan, transaction-processing policies, third-party description or other existing R-1900 materials. The fields can also be satisfied by a clear cross-reference to existing enterprise documentation. This approach gives reviewers consistent information without requiring the Board to administer a separate non-mandatory annex.

Question 15: burden reduction through reuse and stable identifiers—Each material dependency can be assigned a stable identifier so later submissions report only changes. Applicants should be permitted to cross-reference existing enterprise architecture, third-party risk, operational-resilience and BSA/AML documentation rather than restate it. In a consortium, common technical facts can be stated once, but every applicant should identify which common facts it adopts and provide its own legal, governance, financial-support and responsibility information.

Implementation during a pending application—The standardized dependency fields should be versioned and owned by a named function. Each change should record the date, reason, reviewer, effect on the dependency tier and whether information previously submitted to the Board remains sufficient. The same control owner should connect the change record to the Standards and Issue Review Register described above, so that new standards, cyber findings, recurring defects and provider incidents can be assessed consistently. Changes that do not affect the sufficiency of the statutory-factor record can remain in ordinary governance and guidance channels; changes that may affect a statutory factor should be escalated for application supplementation and, where appropriate, pre-filing or supervisory discussion. This preserves a living control record without treating every operational update as a new filing.

Question 7: pre-filing for novel or high-risk dependencies—R-1900 notes the Federal Reserve's existing pre-filing process for complex proposals. Applicants with high-risk external-event triggers, unusual governance rights, novel lawful-order intervention constraints, or multi-regulator consortium structures can use pre-filing to agree on the level of supporting detail before preparing extensive documentation. This can reduce burden for both applicants and reviewers.¹

10. Conclusion

R-1900 already asks for most of the information needed to review a stablecoin business model that depends on external commercial events. The most useful refinement is not a new supervisory mandate or a new filing artefact. It is a disciplined way to make a material dependency visible inside the information the Board already requests and to show that the applicant has a durable governance process for keeping that information current. A reviewer should be able to see what external status can affect a financial action, who controls the relevant decision path, which internal function is accountable, what issuer-level intervention remains available, how the transaction is reconciled, how standards and cyber risks are periodically challenged, how recurring problems are mapped and remediated, and which legal entity owns the dependency and resulting loss pathway. The reviewer need not determine whether the underlying trade event itself was commercially correct.

DigitalTrade4.EU therefore recommends that the Board:

1. clarify that review of material external-event and attestation dependencies concerns the PPSI control environment, accountability and resilience, not Federal Reserve validation of underlying trade facts or documents;
2. use a concise set of standardized external-dependency fields within existing R-1900 materials, with cross-reference to existing controls where possible, rather than create a separate optional annex;
3. calibrate the level of dependency detail to risk while keeping any qualitative tier distinct from R-1899 capital requirements and supervisory ratings;
4. clarify proposed § 247.30(c)(2) with non-exclusive technical examples focused on whether a change makes the statutory-factor record insufficient;
5. in consortium structures, permit reuse of common technical facts while preserving each applicant's adoption, certification, governance, financial-support and responsibility record;
6. where external triggers can affect payment or redemption, require clear issuer-controlled intervention, compromised-attester quarantine, exception, continuity and reconciliation controls, with the pre-finality/post-finality boundary made explicit; and
7. for multiple stablecoins under Question 17, use a common-baseline plus token-specific Delta Schedule to show what is unchanged and what requires additional review.
8. require a clear internal accountability chain for material dependencies, including accountable ownership, decision rights, independent challenge, override authority, escalation, continuity and responsibility for material-change screening; and
9. expect a risk-based continuous-monitoring and periodic-review process for material standards, interoperability and cybersecurity assumptions, supported by structured issue mapping, root-cause remediation, updated guidance and controlled information sharing, while reserving regulatory supplementation for changes that affect the sufficiency of the statutory-factor record.

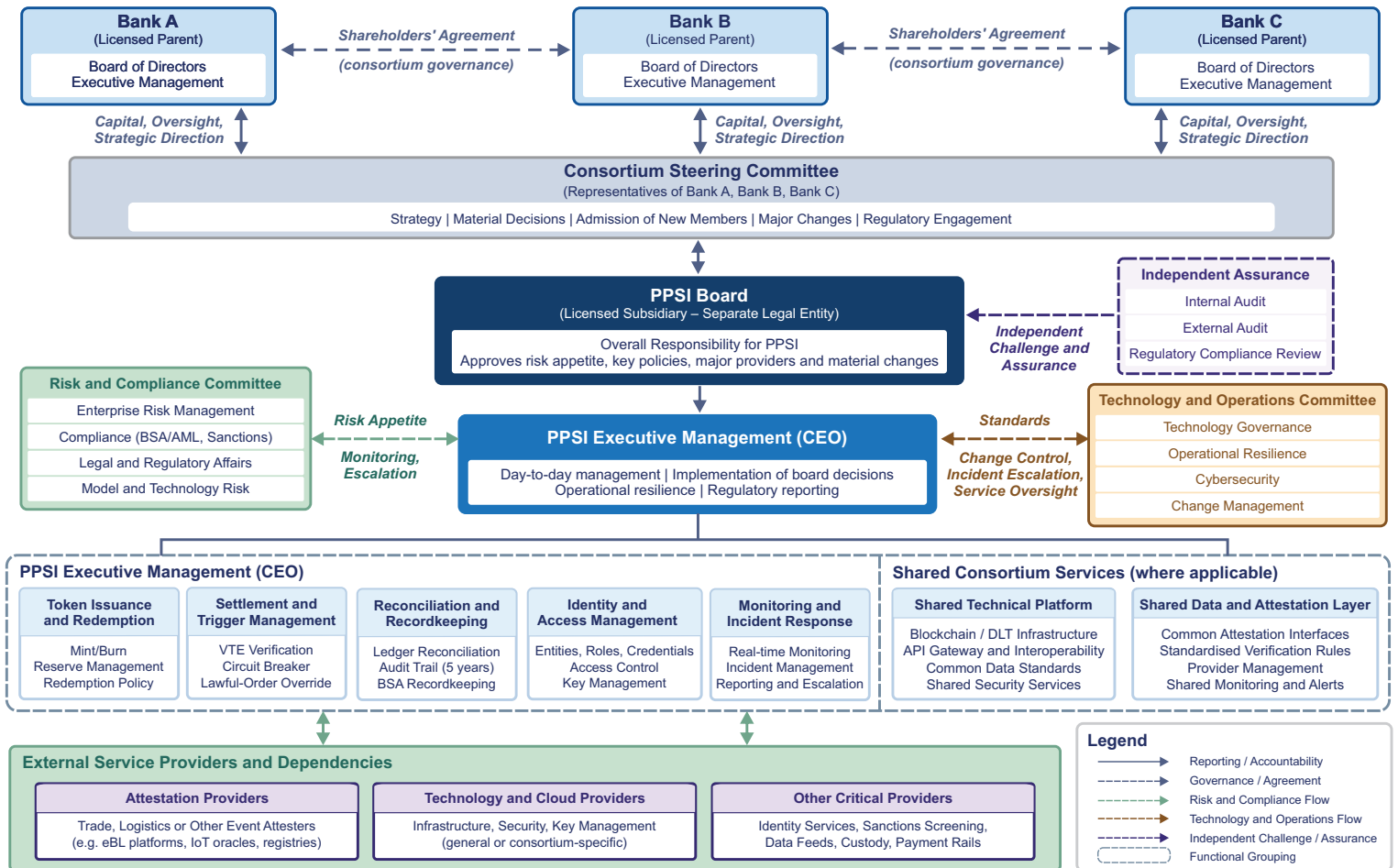
These steps would preserve R-1900's technology-neutral and tailored application approach, align the information request with the Board's statutory role, and make novel payment architectures easier to review without expanding the Board into trade-document adjudication.

Notes and References

1. Board of Governors of the Federal Reserve System. “Application Procedures for Board-Supervised Insured Depository Institutions Seeking Approval for a Subsidiary to Issue Payment Stablecoins.” Docket No. R-1900, RIN 7100-AH30, Notice of Proposed Rulemaking, 24 September 2026. <https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20260924a3.pdf>
2. Board of Governors of the Federal Reserve System. “Implementing the Federal Reserve Board’s Responsibilities under the GENIUS Act.” Docket No. R-1899, RIN 7100-AH29, Notice of Proposed Rulemaking, 24 September 2026. The proposal includes the Board’s proposed operational-risk capital framework, historical-loss scalar, operational-loss data requirements, and discussion of technological capability to comply with lawful orders. <https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20260924a4.pdf>
3. Financial Crimes Enforcement Network. 31 CFR § 1010.430, Nature of records and retention period. Records required under applicable BSA regulations are generally subject to specified retention requirements, commonly five years; the applicability of a retention rule depends on the record at issue. <https://www.ecfr.gov/current/title-31/subtitle-B/chapter-X/part-1010/subpart-D/section-1010.430>
4. Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS Act), Pub. L. No. 119-27, 139 Stat. 419, codified at 12 U.S.C. 5901 et seq. R-1900 cites the statutory provisions governing application review, statutory factors, completeness, timing and material change.
5. Federal Reserve Board. R-1900 proposal and public-comment submission page. <https://www.federalreserve.gov/apps/forms/proposals/FR-2026-0034-01>
6. DigitalTrade4EU. “Towards a Trusted Digital Trade Framework: The Role of the European Trade Indexes Registry (EUTIR): Summary of Feedback to the European Commission.” September 2025, v8.11 [GLOBAL]. See Annex II §§ 6–7 on supervision, incident reporting and framework review, and the Common Technical Specifications on versioning and maintenance. This prior research is cited only as a governance-design precedent; its EU institutional structure is not proposed for transplantation into R-1900.

Appendix A. Illustrative Consortium Governance and Accountability Structure

Organisational hierarchy, decision rights and information flows for a consortium-based Payment Stablecoin Issuer (PPSI)



Illustrative only. This diagram does not propose a mandatory governance structure. It shows one possible allocation of accountability, decision rights, independent challenge and shared-service relationships in a consortium-based PPSI while preserving the legal responsibility of the licensed entity.

Appendix B

The following fields are an illustrative information structure for a material external dependency. They are designed to be embedded in or cross-referenced from the business plan, policies, third-party materials or other information already submitted under R-1900. They are not intended to prescribe a separate annex, a specific architecture, data standard, capital treatment or legal characterization.

Table 7. Illustrative embedded External Dependency disclosure fields.

Field	Illustrative content
1. Dependency ID / accountable owner	Stable identifier; accountable PPSI or applicant function; any common infrastructure owner separately identified.
2. Use case and statutory mapping	Product/service; affected transaction stage; relevant §5(c) factor and R-1900 application evidence.
3. External status / condition	External condition recognized by the PPSI and financial consequence if accepted, rejected, delayed or disputed; no Fed adjudication of the underlying trade fact.
4. Evidence reference and source	Record/message/source identifier; whether PPSI receives source data, a reference or only an attestation.
5. Verification / attestation	Verifier, verification rule, credential/trust basis and resulting status.
6. Identity and authority	How actor identity and authority to make or attest the statement are established, limited and revoked.
7. Interface / standard	API, schema, messaging standard, event identifier, ledger reference or other interface.
8. Disclosure tier	Low / Medium / High application-detail tier, with brief rationale; not a capital or supervisory rating.
9. Settlement / redemption effect	How the external status changes payment, settlement or redemption processing.
10. Intervention / lawful-order control	Issuer-controlled points to suspend, quarantine, reject or otherwise intervene; compromised-attester circuit breaker; pre-finality and post-finality capabilities.
11. Integrity and lifecycle	Sequencing, freshness, duplicate prevention, correction, revocation, disputes and stale-data handling.
12. Reconciliation and audit	Transaction-to-event reference, decision timestamp, exception history and records needed to reconstruct the processing path.
13. Record-retention classification	Applicable BSA/AML, supervisory, legal, contractual or operational retention category and accessibility requirement.
14. Continuity / fallback	Action if source, verifier, credential or interface is unavailable, inconsistent or compromised.
15. Control / governance rights	Who can change rules, providers, keys, participant eligibility or transaction logic; relevant veto or approval rights.

16. Financial support / loss pathway	Legal entity bearing guarantee, indemnity, service obligation or remediation cost; plausible operational-loss pathway.
17. Change trigger	Changes that require field update, application supplementation or materiality escalation under proposed §247.30(c)(2).
18. Internal accountability	Accountable owner, control owner, override authority, independent challenge, escalation path and responsible application/material-change owner.
19. Standards and cybersecurity review	Relevant standards/threat sources; review owner; risk-based cadence; last review; compatibility or cyber findings; planned migration/remediation; event-driven review triggers.
20. Issue and guidance register	Recurring issue or near miss; affected dependency/standard; impact; root cause; workaround; remediation; owner; updated guidance/control; closure evidence.
21. Information sharing and management reporting	Upward: incidents, unresolved gaps, override events, repeated reconciliation breaks, significant standards/cyber changes and material-change decisions. Horizontal: implementation guidance and lessons for affected technology, operations, risk, compliance, legal and relevant consortium/provider functions. Supervisory: required reporting and R-1900 supplementation where previously submitted information is no longer sufficient; include confidentiality and distribution controls.