SETTLEMENT INTEGRITY INSTITUTE

SII

THE STANDARD FOR TOKENIZED VALUE ASSURANCE

GLOSSARY

Version 1.0

The infrastructure of trust for tokenized value settlement.

MAY 12, 2026

Preface

A glossary, properly understood, is not a dictionary. A dictionary records the senses in which a word is in fact used; a glossary establishes the senses in which a word is to be used within the discipline that publishes it. The distinction matters. When practitioners, regulators, and counterparties to a settlement system use a term in different senses, the consequence is not linguistic confusion — it is the silent failure of the assurance the term was meant to convey.

This glossary defines the terms that the Settlement Integrity Institute uses, and intends to use consistently, in its assessment of tokenized settlement infrastructure. The terms are not new vocabulary invented for the occasion. Each either already appears in published SII canon or names a structural feature that the doctrine requires and that the regulatory and standards literature describes without naming. The work of the glossary is to fix the meaning of these terms with the precision that an assurance discipline requires.

Two editorial commitments shape what follows. *The glossary defines what only SII can define.* Terms adequately settled by FATF, IOSCO, ISO, MiCA, the GENIUS Act, the NRSRO framework, and the CPMI-IOSCO Principles for Financial Market Infrastructures are intentionally omitted, because their definitions are not ours to render. *References are load-bearing only.* Each citation anchors a term against an originating instrument, distinguishes it from a concept being refined, or links it to a dependent SII term.

The glossary is organized in three groups. **Foundations** establish the conceptual spine of the doctrine — the terms without which the framework does not stand. **Operations** supply the working vocabulary an analyst, regulator, or counterparty needs to discuss settlement infrastructure with precision. **Distinctions** resolve conflations the field's vocabulary has produced and which obscure the questions that matter.

This is version 1.0. The doctrine the glossary expresses will continue to develop as tokenized settlement infrastructure matures and as the regulatory architecture around it takes shape. Subsequent versions will record those developments transparently and will preserve a clear record of what has changed and why. The terms defined here, however, are intended to hold.

How to Use This Glossary

Each entry has the same structure. The **Definition** is the canonical statement of the term, intended to be quotable as a single block. The **Notes** carry the load — they place the term in its institutional context, name the regulatory or standards literature it draws on or distinguishes itself from, and identify what only this term names. The **See also** block links to other terms in the glossary that share doctrinal weight with the entry. The **References** anchor the entry against external instruments.

For citation in regulatory filings, academic work, or institutional analysis, see the citation format below. For navigation, the entries can be read in canonical order — Group I through Group III — or accessed individually through the cross-reference graph. Every term referenced in a *See also* block is itself a defined term in this glossary.

The glossary is published as a PDF of record. The PDF is the canonical artifact.

Citation Format

Entries from this glossary should be cited in the following form:

> *Settlement Integrity Institute, Glossary v1.0, s.v. "[term]" (May 2026).*

For example:

> *Settlement Integrity Institute, Glossary v1.0, s.v. "Operational Suitability" (May 2026).*

Version Policy

This glossary is published as version **1.0** on **May 12, 2026.**

Subsequent versions will be released as the doctrine develops. The Institute's version policy is as follows:

- **Minor versions** (1.x) introduce calibrations, clarifications, or additions that do not displace prior definitions. Existing terms continue to apply.
- **Major versions** (2.0, 3.0) introduce changes that materially alter a prior definition. Such changes are explicitly noted, with the prior definition preserved in an archival appendix.
- **Term retirements**, where they occur, are noted and explained. A term once defined here is not silently withdrawn.

The Institute maintains a change log alongside each release. Citations should specify the version (e.g., *Glossary v1.0*) so that the applicable definition is unambiguous on the date of citation.

Comment, correction, and contribution are welcomed at comments@siistandards.com.

GROUP I

Foundations

The conceptual spine of the doctrine. Without these, the framework does not stand.

1. Trust Fabric
2. Operational Suitability
3. Settlement Finality
4. Assurance Gap
5. Tokenized Value Settlement
6. Deterministic Behavior

Trust Fabric

GLOSSARY OF THE SETTLEMENT INTEGRITY INSTITUTE · V1.0 · GROUP I — FOUNDATIONS

DEFINITION

The composite of legal, operational, custodial, technical, and governance arrangements that together determine whether a settlement system can be relied upon to deliver value with finality, under stress, across jurisdictions and counterparties. Trust Fabric is not a single component, a single party, or a single jurisdiction's regulatory regime. It is the integrated condition produced when all of these elements hold simultaneously.

NOTES

Where U.S. regulators have clarified the *permissibility* of bank participation in tokenized settlement,[1] they have not — and do not purport to — define the fabric within which that participation must hold together. International standard-setters describe such a fabric without naming one.[2,3] Trust Fabric supplies the name.

The term carries three operational properties. *Fabric* implies weave: the strength of the system is the strength of the weakest binding between elements, not the strength of the strongest element. *Trust is conferred, not asserted* — it is the output of a system that has been examined, not a property an issuer can claim. *Fabric implies inspectability:* a fabric can be tested at any point, and a tear in one place compromises the whole.

SEE ALSO

Operational Suitability · Infrastructure Trust Boundary · Assurance Gap · Methodology Authority · Settlement Substrate

REFERENCES

1. Office of the Comptroller of the Currency, *Interpretive Letter 1183: Letter Addressing Certain Crypto-Asset Activities* (March 7, 2025). occ.gov
2. Financial Stability Board, *High-level Recommendations for the Regulation, Supervision and Oversight of Global Stablecoin Arrangements: Final Report* (July 17, 2023). fsb.org
3. Committee on Payments and Market Infrastructures & International Organization of Securities Commissions, *Application of the Principles for Financial Market Infrastructures to Stablecoin Arrangements* (July 13, 2022). bis.org

Operational Suitability

GLOSSARY OF THE SETTLEMENT INTEGRITY INSTITUTE · V1.0 · GROUP I — FOUNDATIONS

DEFINITION

A determination that a settlement infrastructure — taken as a whole — is fit to bear the value, volume, counterparty exposure, and stress conditions placed upon it. Operational Suitability is established by examination of the infrastructure's components, their bindings, and the conditions under which they have been observed to hold; it is not established by attestation, certification of any single component, or compliance with rules governing parts of the system in isolation.

NOTES

Existing supervisory frameworks examine operational risk *within* a regulated institution. The OCC Heightened Standards govern risk governance inside large national banks;[1] the FFIEC IT Examination Handbook prescribes how an institution oversees its third-party technology providers;[2] the Basel Committee's *Principles for Operational Resilience* set expectations for how a bank withstands disruption.[3] Each is indispensable, and none was designed to evaluate a settlement system whose components span multiple institutions, jurisdictions, and trust regimes simultaneously. Operational Suitability is the cross-component determination those frameworks presume but do not themselves render.

The determination is *of the whole*: a settlement infrastructure whose individual components are each in compliance with their applicable rules may still be operationally unsuitable if the bindings between them are weak, untested, or undocumented. Conversely, an infrastructure whose components are unfamiliar to traditional supervisory frameworks may be operationally suitable where those bindings are demonstrably sound. Suitability is the property of the system, not the property of any participant in it.

SEE ALSO

Trust Fabric · Infrastructure Trust Boundary · Assurance Gap · Methodology Authority

REFERENCES

1. Office of the Comptroller of the Currency, *Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches* (12 C.F.R. Part 30, Appendix D). occ.gov
2. Federal Financial Institutions Examination Council, *FFIEC Information Technology Examination Handbook — Architecture, Infrastructure, and Operations Booklet* (June 2021). occ.gov
3. Basel Committee on Banking Supervision, *Principles for Operational Resilience*, BCBS 516 (March 2021). bis.org

Settlement Finality

GLOSSARY OF THE SETTLEMENT INTEGRITY INSTITUTE · V1.0 · GROUP I — FOUNDATIONS

DEFINITION

The point at which the transfer of value through a settlement system becomes irrevocable, unconditional, and legally enforceable against all participants, the system operator, and any insolvency administrator of any participant. A transfer that can be unwound, reversed, or rendered ineffective by the failure of a participant, the action of a court, or the operation of a system rule has not achieved finality, regardless of how complete it appears on the system's ledger.

NOTES

Settlement finality is a property defined by three established frameworks. The CPMI-IOSCO *Principles for Financial Market Infrastructures* require that a financial market infrastructure provide clear and certain final settlement at a minimum by the end of the value date.[1] The EU Settlement Finality Directive establishes the legal enforceability of transfer orders entered into a designated system, including against an insolvent participant.[2] Article 4A of the Uniform Commercial Code defines the moment a payment order between U.S. banks becomes final and the obligations and rights that attach at that moment.[3] Together, these frameworks define what finality *means* and the conditions under which it may be relied upon — for the institutions and instruments they were designed to govern.

Tokenized value settlement raises questions these frameworks did not anticipate. *On-chain confirmation is not finality.* A confirmed transaction may be legally reversible if the underlying obligation was never enforceable, the issuer's redemption duty has not been satisfied, or the chain itself is subject to reorganization. *Probabilistic settlement is not finality.* A transaction whose irrevocability depends on the continued cooperation of a validator set is not unconditional within the meaning of the established frameworks. *Off-chain reserve adequacy is not finality.* A token whose redemption can be suspended, gated, or conditioned has not achieved finality at the moment of transfer. The question for tokenized settlement is not whether finality applies — it does — but at what point, on what conditions, and against what counterparties it has been achieved.

SEE ALSO

Trust Fabric · Operational Suitability · Tokenized Value Settlement · Deterministic Behavior · Settlement vs. Clearing

REFERENCES

1. Committee on Payments and Market Infrastructures & International Organization of Securities Commissions, *Principles for Financial Market Infrastructures*, Principle 8 (April 2012). iosco.org

2. Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on settlement finality in payment and securities settlement systems. eur-lex.europa.eu
3. Uniform Commercial Code Article 4A — Funds Transfers. law.cornell.edu

Assurance Gap

GLOSSARY OF THE SETTLEMENT INTEGRITY INSTITUTE · V1.0 · GROUP I — FOUNDATIONS

DEFINITION

The structural deficit that exists when a settlement system has no recognized authority capable of rendering an integrated determination of its operational suitability across all components, jurisdictions, and trust regimes on which it depends. The Assurance Gap is not a deficiency of any individual regulator, supervisor, auditor, or rating agency; it is the absence of a mechanism by which their separate determinations can be composed into a single, defensible assessment of the system as a whole.

NOTES

The President's Working Group on Financial Markets identified the structural feature in 2021: stablecoin oversight is *"inconsistent and fragmented, with some stablecoins effectively falling outside the regulatory perimeter."*[1] The Financial Stability Board identified the same feature again in 2025, finding *"significant gaps and inconsistencies"* in the implementation of its global stablecoin recommendations and warning that fragmented oversight creates opportunities for regulatory arbitrage.[2] Each of these findings describes the symptom. The Assurance Gap names the underlying structural condition that produces it.

The gap exists in three dimensions simultaneously. *Across components*, no authority assesses the issuer, custodian, validator set, oracle network, and redemption pathway as a single integrated system. *Across jurisdictions*, no authority renders a determination that binds across the legal regimes a tokenized settlement actually traverses. *Across trust regimes*, no authority bridges the supervisory frameworks built for regulated institutions and the operational realities of infrastructure that includes unregulated participants. Closing the gap requires an institution whose mandate is precisely this composition — not a deeper regulator, a broader supervisor, or a more sophisticated auditor, but a different *kind* of authority.

SEE ALSO

Trust Fabric · Operational Suitability · Methodology Authority · Black-Box Infrastructure

REFERENCES

1. President's Working Group on Financial Markets, Federal Deposit Insurance Corporation, and Office of the Comptroller of the Currency, *Report on Stablecoins* (November 1, 2021). home.treasury.gov
2. Financial Stability Board, *Thematic Peer Review on the FSB Global Regulatory Framework for Crypto-asset Activities* (October 16, 2025). fsb.org
3. Financial Stability Board, *High-level Recommendations for the Regulation, Supervision and Oversight of Global Stablecoin Arrangements: Final Report* (July 17, 2023). fsb.org

Tokenized Value Settlement

GLOSSARY OF THE SETTLEMENT INTEGRITY INSTITUTE · V1.0 · GROUP I — FOUNDATIONS

DEFINITION

The transfer of value through a settlement system in which the unit of value is represented by a digital token issued, recorded, and conveyed on a distributed ledger or comparable programmable platform, and in which the obligations of the issuer, the custodial arrangements for any underlying reserve, and the operational behavior of the platform together determine whether the transfer constitutes a final settlement of the underlying claim.

NOTES

Tokenized value settlement is not a single architecture. The unit of value may be a payment stablecoin redeemable at par against a reserve of high-quality liquid assets, as defined under the GENIUS Act;[1] a tokenized deposit representing a claim against an insured depository institution; a wholesale central bank money token used for interbank settlement;[2] or a tokenized security representing an interest in an underlying instrument.[3] Each architecture distributes the obligations of issuance, custody, conveyance, and redemption differently, and each composes a different settlement system around the token.

What is common across architectures is that *the token is not the value*. The token is a representation of a claim against an issuer, supported by reserves under the control of a custodian, conveyed across a platform operated by participants who are themselves subject to (or absent from) supervisory frameworks. Whether a transfer of the token constitutes settlement of the underlying claim depends on the integrity of every link in that chain. Tokenized value settlement is therefore not the act of moving a token; it is the condition produced when the act of moving a token produces final settlement of the value the token represents.

SEE ALSO

Trust Fabric · Settlement Finality · Reserve Custody Architecture · Redemption Pathway · Settlement Substrate

REFERENCES

1. Guiding and Establishing National Innovation for U.S. Stablecoins (GENIUS) Act of 2025, § 2(22) (definition of "payment stablecoin") and § 4(a)(1)(A) (permissible reserve assets). paulhastings.com
2. Bank for International Settlements, *Wholesale Central Bank Money in the Context of Tokenisation* (September 16, 2025). bis.org
3. Board of Governors of the Federal Reserve System, *Capital Treatment of Tokenized Securities — Frequently Asked Questions* (March 5, 2026). federalreserve.gov

Deterministic Behavior

GLOSSARY OF THE SETTLEMENT INTEGRITY INSTITUTE · V1.0 · GROUP I — FOUNDATIONS

DEFINITION

The property of a settlement system, or any component of one, that the same input produces the same output every time the operation is performed, by every participant who performs it, under every condition the system is designed to encounter. Deterministic behavior is what makes the operation of a settlement system inspectable, testable, and reliable — and what distinguishes engineered settlement infrastructure from systems whose outcomes vary with circumstance, party, or time.

NOTES

In the context of distributed ledger systems, deterministic behavior is a technical requirement: every node executing the same transaction against the same state must arrive at the same result, or consensus fails and the ledger forks. This is the operational meaning of determinism that the engineering literature treats as foundational.

For settlement infrastructure as a whole, the requirement extends beyond the execution layer. *Reserve operations* must produce the same redemption outcome regardless of which authorized party initiates them. *Custodial release* must follow the same procedure regardless of which counterparty stands behind the claim. *Stress responses* must follow predetermined rules rather than discretionary judgments rendered in the moment. A settlement system whose behavior is deterministic at the chain layer but discretionary at the institutional layer has not achieved deterministic behavior — it has merely localized it.

The standards bodies have built vocabulary for the technical layer. The ISO 23257 reference architecture for distributed ledger technology specifies the functional components and behaviors required for DLT systems to operate predictably.[1] The NIST glossary defines smart contracts as collections of code and data executing on a blockchain.[2] ESMA's MiCA technical standards prescribe deterministic record-keeping and message formats for crypto-asset service providers.[3] What none of these address is the question that matters for settlement: whether the *system as a whole* — including its institutional and custodial layers — exhibits the same property the chain layer is required to exhibit. Deterministic behavior in the SII sense is the system-level extension.

SEE ALSO

Trust Fabric · Operational Suitability · Settlement Finality · Programmable Compliance · Black-Box Infrastructure

REFERENCES

1. International Organization for Standardization, *ISO 23257:2022 — Blockchain and distributed ledger technologies — Reference architecture* (February 2022). iso.org
2. National Institute of Standards and Technology, *Computer Security Resource Center Glossary — "Smart contract."* csrc.nist.gov
3. European Securities and Markets Authority, *Statement on the Smooth Implementation of MiCA Data Standards and Format Requirements*, in *Markets in Crypto-Assets Regulation (MiCA)* technical standards. esma.europa.eu

GROUP II

Operations

The operational vocabulary an analyst, regulator, or counterparty needs to discuss settlement infrastructure precisely.

1. Substantial Similarity
2. Operational Readiness Assessment
3. Infrastructure Trust Boundary
4. Reserve Custody Architecture
5. Redemption Pathway
6. Chain-Level Dependency
7. Validator Concentration Risk
8. Key Management Regime
9. Settlement Recovery
10. Programmable Compliance
11. Cross-Chain Settlement
12. Black-Box Infrastructure
13. Methodology Authority
14. Recertification Cycle
15. Settlement Substrate

Substantial Similarity

GLOSSARY OF THE SETTLEMENT INTEGRITY INSTITUTE · V1.0 · GROUP II — OPERATIONS

DEFINITION

A determination that a foreign or alternative regulatory and supervisory regime produces outcomes equivalent to a designated U.S. regime, evaluated against the substantive standards the U.S. regime imposes — not the form, label, or procedural design through which that regime delivers them.

NOTES

In the payment stablecoin context, the term derives from Section 18 of the GENIUS Act and 12 U.S.C. § 5916, which condition foreign-issuer access to U.S. markets on a Treasury determination that the foreign regime is *comparable* to the standards established under 12 U.S.C. § 5903(a).[1] Treasury's implementing rulemaking reads the statutory phrase as a *substance* test: deviations in form or procedure do not, by themselves, defeat a finding of comparability where the foreign regime meets or exceeds the U.S. substantive standards.[2]

A substantial similarity determination is not a rating, a treaty obligation, or a passport. It is a unilateral, rescindable determination by the U.S. authority, made on a regime-by-regime basis and conditioned on continued comparability. A regime that drifts loses recognition; a regime that hardens may earn it.

SEE ALSO

Operational Suitability · Methodology Authority · Trust Fabric

REFERENCES

1. 12 U.S.C. § 5916 — Exception for foreign payment stablecoin issuers and reciprocity for payment stablecoins issued in overseas jurisdictions. uscode.house.gov
2. U.S. Department of the Treasury, *Notice of Proposed Rulemaking: Principles for Substantial Similarity Determinations under the GENIUS Act*. home.treasury.gov

Operational Readiness Assessment

GLOSSARY OF THE SETTLEMENT INTEGRITY INSTITUTE · V1.0 · GROUP II — OPERATIONS

DEFINITION

The structured examination of a settlement infrastructure — its components, bindings, controls, and stress responses — undertaken to render an integrated determination of whether the infrastructure is fit to operate at the value, volume, and counterparty exposure represented to its participants. An Operational Readiness Assessment evaluates the system as a whole; it is not a sum of attestations covering its parts.

NOTES

The assessment is examined, not asserted. Issuer self-attestation, custodian SOC reports, smart-contract audits, and chain-level certifications are inputs to an Operational Readiness Assessment; none, individually or in combination, constitutes one. The assessment exists to produce a determination — a statement, by an authority with the standing to make it, that the integrated system meets the operational suitability criteria the infrastructure must satisfy. It is the procedural counterpart to Operational Suitability: the *how* by which the *what* is determined.

The Federal financial institution agencies have built an extensive supervisory examination apparatus for the institutions they supervise — the FFIEC IT Examination Handbook,[1] the Interagency Guidance on Third-Party Relationships,[2] and the FFIEC Business Continuity Management booklet[3] together prescribe how an examiner evaluates technology, third-party reliance, and resilience inside a regulated institution. An Operational Readiness Assessment of a tokenized settlement infrastructure draws on these examination disciplines but applies them at the layer they were not designed for: the integrated multi-party system whose components span institutions, jurisdictions, and trust regimes.

SEE ALSO

Operational Suitability · Trust Fabric · Recertification Cycle · Methodology Authority

REFERENCES

1. Federal Financial Institutions Examination Council, *FFIEC Information Technology Examination Handbook*. occ.gov
2. Board of Governors of the Federal Reserve System, FDIC, and OCC, *Interagency Guidance on Third-Party Relationships: Risk Management* (June 6, 2023). federalreserve.gov
3. Federal Financial Institutions Examination Council, *FFIEC IT Examination Handbook — Business Continuity Management Booklet* (November 2019). occ.gov

Infrastructure Trust Boundary

GLOSSARY OF THE SETTLEMENT INTEGRITY INSTITUTE · V1.0 · GROUP II — OPERATIONS

DEFINITION

The defined perimeter within which a Trust Fabric has been examined and is held to operate as a single integrated settlement system. Inside the boundary, the components, bindings, and conditions of operation are known and have been tested. Outside the boundary, no determination has been made and no reliance is warranted.

NOTES

A boundary is what makes a Trust Fabric assessable. Without one, the question *is this infrastructure trustworthy?* has no defensible answer, because the scope of *this* is unspecified. The boundary names what was examined, what was not, and where the determination ceases to apply.

Boundaries are drawn along three axes — *components* (which issuers, custodians, validators, oracles, redemption pathways are within scope), *jurisdictions* (which legal regimes' rules govern the assessment), and *operating conditions* (the value, volume, and stress envelopes under which the determination holds). A change to any axis — a new sub-custodian, a new chain, a stress condition outside the tested envelope — is a change to the boundary, and may require recertification before the determination continues to apply.

SEE ALSO

Trust Fabric · Operational Suitability · Recertification Cycle · Chain-Level Dependency

REFERENCES

1. Office of the Comptroller of the Currency, *Interpretive Letter 1183: Letter Addressing Certain Crypto-Asset Activities* (March 7, 2025). occ.gov
2. Board of Governors of the Federal Reserve System, FDIC, and OCC, *Interagency Guidance on Third-Party Relationships: Risk Management* (June 6, 2023). federalreserve.gov

Reserve Custody Architecture

GLOSSARY OF THE SETTLEMENT INTEGRITY INSTITUTE · V1.0 · GROUP II — OPERATIONS

DEFINITION

The arrangement of legal, operational, and technical controls under which the assets backing a tokenized claim are held, segregated, accounted for, and made available for redemption. A Reserve Custody Architecture is not a single account or a single custodian; it is the composition of legal segregation, operational segregation, sub-custodial relationships, and reconciliation procedures that together determine whether the reserve, as held, can satisfy the redemption duty as owed.

NOTES

For payment stablecoins, the GENIUS Act prescribes the *composition* of permissible reserves — U.S. currency, insured depository deposits, short-dated Treasuries, overnight repos, government money market fund shares, and tokenized forms of the foregoing[1] — and the OCC's implementing rulemaking prescribes how those reserves must be held by OCC-supervised custodians.[2] Together, the statute and the rule answer two of the three questions a Reserve Custody Architecture must resolve: *what assets count*, and *how they must be held by a supervised custodian.*

The third question — *whether the architecture, as composed, satisfies the redemption duty* — is not answered at the asset or custodian layer. It is answered at the architectural layer: by the chain of custody between issuer, custodian, sub-custodian, and any tokenization platform; by the legal segregation that protects the reserve from the issuer's bankruptcy estate;[3] by the reconciliation procedures that bind on-chain supply to off-chain reserves; and by the operational latency between a redemption request and the release of the underlying asset. A Reserve Custody Architecture either resolves these questions or it does not. Compliance with the asset and custodian rules is necessary but not sufficient.

SEE ALSO

Tokenized Value Settlement · Redemption Pathway · Settlement Finality · Custody vs. Custodianship

REFERENCES

1. Guiding and Establishing National Innovation for U.S. Stablecoins (GENIUS) Act of 2025, § 4(a)(1)(A). paulhastings.com
2. Office of the Comptroller of the Currency, *Proposed Rule: Implementation of the GENIUS Act — Custody, Reserve, Capital, and Risk Management Requirements*. nixonpeabody.com
3. GENIUS Act, § 11(d)–(e), amending 11 U.S.C. §§ 507(e) and 541(b)(11) (super-priority for stablecoin holders; reserves excluded from the bankruptcy estate). paulhastings.com

Redemption Pathway

GLOSSARY OF THE SETTLEMENT INTEGRITY INSTITUTE · V1.0 · GROUP II — OPERATIONS

DEFINITION

The end-to-end operational route by which a holder of a tokenized claim converts that claim back into the underlying asset at par, including every intermediary, control, latency, and condition that gate the conversion. A Redemption Pathway is defined by its narrowest point under stress, not by its capacity in ordinary conditions.

NOTES

Redemption is the property a tokenized claim is *for*. A token whose redemption is conditional, gated, suspendable, or operationally fragile has not preserved the claim it represents — it has substituted a new claim with weaker properties. The Redemption Pathway is the unit of analysis through which the strength of that preservation is examined.

The pathway is examined under stress, not under steady state. *In ordinary conditions,* most redemption architectures perform adequately. *In stressed conditions* — concentrated redemption demand, custodian operational failure, banking partner disruption, chain congestion — the pathway's narrowest point determines whether redemption holds. A pathway that admits no narrow point under any plausible stress is sound; a pathway whose narrowest point is unknown is, by definition, not assessable.

SEE ALSO

Reserve Custody Architecture · Settlement Finality · Settlement Recovery · Tokenized Value Settlement

REFERENCES

1. Guiding and Establishing National Innovation for U.S. Stablecoins (GENIUS) Act of 2025, § 4 (reserve and redemption requirements). paulhastings.com
2. Financial Stability Board, *High-level Recommendations for the Regulation, Supervision and Oversight of Global Stablecoin Arrangements: Final Report*, Recommendation 9 (redemption rights). fsb.org

Chain-Level Dependency

GLOSSARY OF THE SETTLEMENT INTEGRITY INSTITUTE · V1.0 · GROUP II — OPERATIONS

DEFINITION

A reliance, by a settlement system, on the continued availability, behavior, governance, or rule-set of a particular distributed ledger or set of ledgers. Chain-Level Dependencies are properties of the *infrastructure that uses the chain*, not of the chain itself, and must be assessed as such.

NOTES

A token issued on a chain depends on that chain. The dependency is not abstract: it includes the chain's continued operation, the stability of its consensus rules, the absence of contentious forks, the behavior of its governance process, and the availability of its bridges, oracles, and middleware. None of these properties are guaranteed by the issuer; all of them condition the issuer's ability to honor the claim represented by the token.

The question for an Operational Readiness Assessment is not *whether* a settlement infrastructure has chain-level dependencies — every tokenized system does — but *whether those dependencies have been identified, scoped, and bounded*. A dependency that has been mapped is manageable. A dependency that is unrecognized is the source of the system's most acute risks.

SEE ALSO

Validator Concentration Risk · Cross-Chain Settlement · Black-Box Infrastructure · Infrastructure Trust Boundary

REFERENCES

1. Bank for International Settlements Innovation Hub, *Project Mariana: Cross-Border Exchange of Wholesale CBDCs Using Automated Market-Makers* (September 28, 2023). bis.org
2. Financial Stability Board, *Thematic Peer Review on the FSB Global Regulatory Framework for Crypto-asset Activities* (October 16, 2025). fsb.org

Validator Concentration Risk

GLOSSARY OF THE SETTLEMENT INTEGRITY INSTITUTE · V1.0 · GROUP II — OPERATIONS

DEFINITION

The exposure of a settlement system to the failure, coordination, or capture of a small number of entities that produce blocks, propose finality, or otherwise determine the canonical state of the underlying ledger. Validator Concentration Risk is a property of the settlement system as composed; it is not mitigated by the nominal decentralization of the chain on which the system operates.

NOTES

Nominal decentralization and operational concentration are different properties. A chain may have thousands of validators on paper while a small number of staking pools, hosting providers, or liquid staking protocols exercise effective control over consensus. The question for assessment is not how many validators exist, but how many independent failure points stand between the system and a loss of finality, censorship of transactions, or reorganization of the canonical chain.[1]

The risk compounds at the settlement layer. A settlement system whose finality depends on a chain whose finality depends on a concentrated validator set has inherited that concentration as its own. Identifying validator concentration is a chain-layer exercise; bearing it is a settlement-layer condition.

SEE ALSO

Chain-Level Dependency · Settlement Finality · Deterministic Behavior

REFERENCES

1. Financial Stability Board, *Thematic Peer Review on the FSB Global Regulatory Framework for Crypto-asset Activities* (October 16, 2025). fsb.org
2. Bank for International Settlements Innovation Hub, *Project Mariana: Cross-Border Exchange of Wholesale CBDCs Using Automated Market-Makers* (September 28, 2023). bis.org

Key Management Regime

GLOSSARY OF THE SETTLEMENT INTEGRITY INSTITUTE · V1.0 · GROUP II — OPERATIONS

DEFINITION

The composition of cryptographic, procedural, and governance controls under which the private keys authorizing transfers, issuances, redemptions, and administrative actions on a settlement system are generated, stored, used, rotated, and recovered. A Key Management Regime determines who can move value, under what conditions, and what happens if a key is compromised, lost, or contested.

NOTES

Cryptographic standards for key management are mature. NIST SP 800-57 prescribes the lifecycle of cryptographic keys;[1] FIPS 140-3 establishes validation requirements for the cryptographic modules in which keys are held.[2] The standards bodies have done the work at the module and lifecycle layer.

What the standards do not prescribe is the *governance regime* under which a settlement system's keys are held. NYDFS guidance for virtual currency custodians begins to fill this gap by requiring segregation, sub-custody approval, and operational controls,[3] but the requirement applies to a single custodian, not to a multi-party settlement system. A Key Management Regime, in the SII sense, is the system-level composition: the policies, the multi-party authorizations, the recovery procedures across institutions, and the failover conditions under which custody of the keys can pass without interrupting the settlement guarantee. It is the governance layer the cryptographic standards presume.

SEE ALSO

Reserve Custody Architecture · Operational Suitability · Custody vs. Custodianship

REFERENCES

1. National Institute of Standards and Technology, *Special Publication 800-57 Part 1, Recommendation for Key Management: Part 1 — General* (Revision 5, May 2020). csrc.nist.gov
2. National Institute of Standards and Technology, *Federal Information Processing Standard 140-3, Security Requirements for Cryptographic Modules* (March 22, 2019). csrc.nist.gov
3. New York State Department of Financial Services, *Industry Letter on Custodial Structures for Customer Protection in the Event of Insolvency* (and related virtual-currency custody guidance). dfs.ny.gov

Settlement Recovery

GLOSSARY OF THE SETTLEMENT INTEGRITY INSTITUTE · V1.0 · GROUP II — OPERATIONS

DEFINITION

The set of pre-defined arrangements by which a settlement system continues to provide its critical services, or winds them down in an orderly manner, when its ordinary operations are disrupted by participant default, operational failure, custodian disruption, or any other condition that exceeds the system's steady-state design envelope.

NOTES

The CPMI-IOSCO recovery framework prescribes that every systemically important financial market infrastructure maintain a comprehensive recovery plan, including the stress scenarios that trigger it, the tools available to address those scenarios, and the governance under which those tools are invoked.[1] The framework was written for FMIs whose participants and operators are themselves regulated and whose recovery toolset is well-understood (loss allocation, replenishment, partial tear-up, position transfer).

Tokenized settlement systems inherit the *requirement* but not the *toolset*. The recovery question for a tokenized arrangement is structurally different: when the issuer fails, when the custodian's banking partner fails, when the chain forks, when the validator set is captured — what continues, what unwinds, and on whose authority? Settlement Recovery, in the SII sense, is the answer to that question made specific to a given Trust Fabric. It is not optional. A settlement system without a defined recovery posture has not been examined; it has only been described.

SEE ALSO

Operational Suitability · Trust Fabric · Redemption Pathway · Reserve Custody Architecture

REFERENCES

1. Committee on Payments and Market Infrastructures & International Organization of Securities Commissions, *Recovery of Financial Market Infrastructures — Revised Report* (July 2017). bis.org
2. Committee on Payments and Market Infrastructures & International Organization of Securities Commissions, *Principles for Financial Market Infrastructures*, Principle 3 (framework for the comprehensive management of risks). iosco.org

Programmable Compliance

GLOSSARY OF THE SETTLEMENT INTEGRITY INSTITUTE · V1.0 · GROUP II — OPERATIONS

DEFINITION

The embedding of regulatory obligations — sanctions screening, transfer restrictions, holder eligibility, reporting triggers, and the like — into the executable logic of a settlement system, such that the obligation is enforced at the moment the transaction is performed rather than evaluated after the fact. Programmable Compliance is a property of the system; it is not a substitute for the legal regime under which the obligation arises.

NOTES

The FATF Travel Rule[1] and the sanctions regimes administered by OFAC and equivalent authorities establish *what* the obligation is. Programmable Compliance is one possible answer to *how* the obligation is satisfied within a tokenized settlement system. Done well, it makes compliance continuous, auditable, and operationally cheaper than retrospective screening. Done poorly, it embeds error at scale, introduces failure modes that are difficult to inspect, and creates the appearance of compliance without the substance.

The assessability question is the one that matters. A compliance regime encoded in smart contracts is only as trustworthy as the inspection regime applied to that code, the governance under which it is changed, the data sources on which it depends, and the failover behavior when those sources fail. Programmable Compliance is therefore not a feature an issuer can claim; it is a property of the system that must be examined in the same way as any other component.

SEE ALSO

Deterministic Behavior · Operational Suitability · Black-Box Infrastructure

REFERENCES

1. Financial Action Task Force, *FATF Recommendation 16 (Wire Transfers / Travel Rule)* and *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (October 2021). fatf-gafi.org
2. Bank for International Settlements, *Project Agorá* (cross-border payments using tokenised commercial bank deposits and central bank money). bis.org

Cross-Chain Settlement

GLOSSARY OF THE SETTLEMENT INTEGRITY INSTITUTE · V1.0 · GROUP II — OPERATIONS

DEFINITION

The transfer of value between participants whose tokenized claims are recorded on distinct distributed ledgers, executed through a bridge, intermediary, atomic-swap mechanism, or interoperability protocol. Cross-Chain Settlement inherits the trust assumptions of every chain it traverses and every mechanism that connects them.

NOTES

A cross-chain transaction is not, in the settlement sense, a single transaction. It is a sequence of transactions on distinct ledgers, bound together by a coordinating mechanism whose own trust properties must be assessed alongside those of the underlying chains. The coordinating mechanism is, in most contemporary architectures, the weakest binding in the system — bridges have been the most consistent point of failure in tokenized settlement, and the FSB's 2025 thematic peer review notes that fragmented oversight of these mechanisms remains a primary source of regulatory arbitrage.[1]

Cross-Chain Settlement is assessable, but only if the assessment is performed at the level of the *combined* system. A determination that each individual chain is operationally suitable does not constitute a determination that a settlement traversing them is operationally suitable. The combined system is the unit of assessment.

SEE ALSO

Chain-Level Dependency · Settlement Finality · Validator Concentration Risk · Black-Box Infrastructure

REFERENCES

1. Financial Stability Board, *Thematic Peer Review on the FSB Global Regulatory Framework for Crypto-asset Activities* (October 16, 2025). fsb.org

2. Bank for International Settlements, *Project Mariana: Cross-Border Exchange of Wholesale CBDCs Using Automated Market-Makers* (September 28, 2023). bis.org

Black-Box Infrastructure

GLOSSARY OF THE SETTLEMENT INTEGRITY INSTITUTE · V1.0 · GROUP II — OPERATIONS

DEFINITION

A component of a settlement system whose behavior cannot be examined, whose dependencies cannot be enumerated, or whose failure modes cannot be mapped — and which therefore cannot be assessed. A Black-Box Infrastructure is not necessarily defective; it is unassessable, which for purposes of an Operational Readiness Assessment is functionally equivalent.

NOTES

Inspectability is a precondition of assurance. A component that produces correct outputs from inputs no one has specified, against logic no one has reviewed, with dependencies no one has documented, may operate adequately for years. The Operational Readiness Assessment makes no determination on it. It is excluded from the Trust Fabric because no one — including its operator — can demonstrate the conditions under which it will continue to behave as it has.

The black box may be a closed-source oracle, an undocumented bridge, a custodian whose internal controls are not made available for examination, or a chain whose governance process operates outside any disclosed framework. The remedy is not to reject the component categorically; it is to require that whatever is required to make it assessable be supplied, or that the component be excluded from the Infrastructure Trust Boundary.

SEE ALSO

Operational Suitability · Infrastructure Trust Boundary · Deterministic Behavior · Chain-Level Dependency

REFERENCES

1. Federal Financial Institutions Examination Council, *FFIEC Information Technology Examination Handbook — Architecture, Infrastructure, and Operations Booklet* (June 2021). occ.gov
2. Board of Governors of the Federal Reserve System, FDIC, and OCC, *Interagency Guidance on Third-Party Relationships: Risk Management* (June 6, 2023). federalreserve.gov

Methodology Authority

GLOSSARY OF THE SETTLEMENT INTEGRITY INSTITUTE · V1.0 · GROUP II — OPERATIONS

DEFINITION

The institutional standing required to publish the methodology by which a class of determinations is rendered, to apply that methodology consistently across subjects, and to be relied upon by third parties — including supervisors, counterparties, and the public — for the determinations so rendered. A Methodology Authority is not a regulator, an auditor, or a rating agency; it is the institutional category that publishes the framework against which others' work is measured.

NOTES

The category is familiar across mature regulatory ecosystems. The Financial Accounting Standards Board publishes the Codification under which U.S. financial reporting is rendered; the International Accounting Standards Board publishes the standards under which non-U.S. reporting is rendered; the Public Company Accounting Oversight Board publishes the auditing standards under which those reports are examined and inspects the firms that apply them.[1] The Nationally Recognized Statistical Rating Organization framework administered by the SEC requires that NRSROs determine ratings according to board-approved methodologies that are publicly available, and that those methodologies be inspected for consistent application.[2] The ISO/IEC 17065 framework prescribes the requirements for any body whose business is certifying products, processes, or services against published specifications.[3]

What unites these institutions is the *separation of methodology from application*. The authority that publishes the methodology is institutionally distinct from the parties whose work it governs and from the regulators whose enforcement it informs. The methodology is the institution's product. Its consistency, its transparency, and its endurance across subjects and time are the institution's standing.

The category exists in U.S. financial reporting (FASB), in international financial reporting (IASB), in audit (PCAOB), in credit ratings (NRSROs), in conformity assessment (ISO/IEC 17065 bodies), and in payment systems standards (PFMI under CPMI-IOSCO). It does not yet exist for the Operational Suitability of tokenized settlement infrastructure. That absence is what defines the Assurance Gap.

SEE ALSO

Assurance Gap · Operational Suitability · Operational Readiness Assessment · Recertification Cycle

REFERENCES

1. Public Company Accounting Oversight Board, *PCAOB Inspections — Basics of Inspections*. pcaobus.org

2. Securities and Exchange Commission, *Nationally Recognized Statistical Rating Organizations*, 17 C.F.R. § 240.17g et seq. ecfr.gov

3. International Organization for Standardization & International Electrotechnical Commission, *ISO/IEC 17065:2012 — Conformity Assessment: Requirements for Bodies Certifying Products, Processes and Services*. iso.org

Recertification Cycle

GLOSSARY OF THE SETTLEMENT INTEGRITY INSTITUTE · V1.0 · GROUP II — OPERATIONS

DEFINITION

The defined cadence at which an Operational Readiness Assessment is renewed, together with the conditions outside that cadence — material changes to components, jurisdictions, or operating envelope — that trigger an interim reassessment. A determination that is not on a Recertification Cycle has a known issue date and an unknown expiration date, and is therefore not a continuing determination.

NOTES

Mature assessment regimes operate on cycles. The PCAOB inspects firms with more than 100 issuer audit clients annually and other registered firms at least triennially.[1] The NRSRO framework requires annual examinations.[2] ISO/IEC 17065 conformity-assessment bodies operate surveillance cycles between full recertifications.[3] Every one of these regimes is built on the recognition that an assessment fixed at a point in time, with no defined cadence and no triggers for interim review, is not an assessment of a continuing condition. It is a snapshot.

A Recertification Cycle is the procedural mechanism by which an Operational Readiness Assessment remains a current determination rather than a historical one. Within the cycle, the determination holds. Outside the cycle, or upon the occurrence of a material change to the Infrastructure Trust Boundary, it does not.

SEE ALSO

Operational Readiness Assessment · Infrastructure Trust Boundary · Methodology Authority

REFERENCES

1. Public Company Accounting Oversight Board, *PCAOB Inspections — Basics of Inspections* (annual or triennial inspection cadence). pcaobus.org
2. Securities and Exchange Commission, Office of Credit Ratings annual examination requirement under Section 15E(p)(3) of the Securities Exchange Act. sec.gov
3. International Organization for Standardization & International Electrotechnical Commission, *ISO/IEC 17065:2012 — Conformity Assessment: Requirements for Bodies Certifying Products, Processes and Services*. iso.org

Settlement Substrate

GLOSSARY OF THE SETTLEMENT INTEGRITY INSTITUTE · V1.0 · GROUP II — OPERATIONS

DEFINITION

The underlying ledger, platform, or programmable infrastructure on which tokenized claims are recorded, conveyed, and settled. The Settlement Substrate is not the issuer, the custodian, or the participants; it is the operating layer beneath them, whose properties — its consensus rules, its governance, its availability, its programmability — condition every transaction the system performs.

NOTES

Substrates differ structurally. A tokenized settlement may operate on a permissioned ledger maintained by a known operator under disclosed governance, on a permissionless chain whose validators are pseudonymous and whose consensus is produced by economic incentives, on a unified-ledger platform of the kind contemplated by the BIS,[1] or on a regulated wholesale settlement network of the kind explored by the New York Fed in the Regulated Liability Network proof of concept.[2] Each substrate carries different finality properties, different governance assumptions, and different recovery options, and each composes a different system around the claims it records.

The substrate is not interchangeable with the system. A single substrate may host many distinct settlement systems; a single settlement system may operate across multiple substrates. The properties of the substrate are inputs to the assessment of the system, not substitutes for it.

SEE ALSO

Trust Fabric · Tokenized Value Settlement · Chain-Level Dependency · Cross-Chain Settlement

REFERENCES

1. Bank for International Settlements, *Annual Economic Report 2023 — Blueprint for the future monetary system: improving the old, enabling the new* (Chapter III, the unified ledger). bis.org
2. Federal Reserve Bank of New York Innovation Center, *Facilitating Wholesale Digital Asset Settlement — Regulated Liability Network Proof of Concept*. newyorkfed.org

GROUP III

Distinctions

Sharp clarifications. Each resolves a conflation observed in the field's vocabulary.

1. Settlement vs. Clearing
2. Custody vs. Custodianship
3. Rating vs. Assessment
4. Standard vs. Framework

Settlement vs. Clearing

GLOSSARY OF THE SETTLEMENT INTEGRITY INSTITUTE · V1.0 · GROUP III — DISTINCTIONS

DEFINITION

Clearing is the process by which obligations between counterparties to a transaction are confirmed, netted, and prepared for discharge — including the calculation of what is owed, the matching of instructions, and, where a central counterparty is interposed, the substitution of the CCP as the counterparty to each side. **Settlement** is the discharge of those obligations through the final transfer of value. Clearing produces an obligation to settle; settlement extinguishes it.

NOTES

The two functions are routinely conflated in discussions of tokenized infrastructure, where a single ledger event is sometimes described as accomplishing both. It does not. *Clearing answers what is owed; settlement answers whether it has been paid.* The distinction is preserved in every mature market structure: the CPMI-IOSCO *Principles for Financial Market Infrastructures* treat central counterparties (clearing) and securities settlement systems and payment systems (settlement) as separate categories of infrastructure, each with its own principles.[1] U.S. securities markets separate the National Securities Clearing Corporation from the Depository Trust Company for the same reason.[2]

The conflation matters because the two functions fail differently and are governed differently. A clearing failure is the failure of a counterparty to meet its obligation; the remedy is the CCP's default waterfall, the close-out of positions, the application of margin and guaranty fund resources. A settlement failure is the failure of the transfer itself to become final; the remedy runs through Settlement Finality, Settlement Recovery, and the legal frameworks that govern when and how a transfer becomes irrevocable. *A system that does both is not relieved of doing either correctly.* Where tokenized infrastructure compresses clearing and settlement into a single event, the assessment must establish that the obligations created by clearing have been properly extinguished by settlement — not that the event has occurred.

SEE ALSO

Settlement Finality · Settlement Recovery · Tokenized Value Settlement · Operational Suitability

REFERENCES

1. Committee on Payments and Market Infrastructures & International Organization of Securities Commissions, *Principles for Financial Market Infrastructures* (April 2012), §1.20 (defining categories of FMI). iosco.org
2. Depository Trust & Clearing Corporation, *DTCC Subsidiaries — NSCC and DTC*. dtcc.com
3. Bank for International Settlements, *Delivery Versus Payment in Securities Settlement Systems* (CPSS, September 1992). bis.org

Custody vs. Custodianship

GLOSSARY OF THE SETTLEMENT INTEGRITY INSTITUTE · V1.0 · GROUP III — DISTINCTIONS

DEFINITION

Custody is the technical condition of holding an asset — the possession of the keys, the control of the wallet, the operational ability to transfer. **Custodianship** is the legal and fiduciary office of holding an asset for the benefit of another — the duties owed to the beneficial owner, the standards of care, the segregation requirements, the obligations on insolvency. Custody describes a state; custodianship describes a relationship.

NOTES

A party may have custody without custodianship — a software process holds keys but owes no duties. A party may have custodianship without sole custody — a qualified custodian may rely on sub-custodians, infrastructure providers, or technology vendors who hold portions of the operational stack. *The keys are where the asset can be moved; the duties are where the asset belongs.* The distinction is foundational in trust and banking law, where the qualified custodian framework under the Investment Advisers Act and the segregation requirements under the Customer Protection Rule attach to the office, not merely to the holding.[1] [2] The OCC's interpretive guidance on cryptocurrency custody by national banks turns on the same point: a bank may hold cryptographic keys for a customer because that activity is the modern form of safekeeping — the office of custodianship — not because possession of keys is itself the regulated activity.[3]

Tokenized settlement infrastructure complicates the distinction because operational custody is distributed across systems that were not designed to be custodians. A multi-signature scheme, a smart contract escrow, a validator set, a bridge — each holds a portion of the operational ability to transfer. The assessment question is not whether the keys are secure; it is whether custodianship has been clearly assigned, the duties are owed by an identifiable party, and the operational architecture supports the discharge of those duties under stress. *Custody can be engineered. Custodianship must be owed.*

SEE ALSO

Reserve Custody Architecture · Key Management Regime · Trust Fabric · Infrastructure Trust Boundary

REFERENCES

1. Securities and Exchange Commission, *Custody of Funds or Securities of Clients by Investment Advisers*, 17 C.F.R. § 275.206(4)-2. ecfr.gov
2. Securities and Exchange Commission, *Customer Protection — Reserves and Custody of Securities*, 17 C.F.R. § 240.15c3-3. ecfr.gov
3. Office of the Comptroller of the Currency, *Interpretive Letter 1170: National Bank and Federal Savings Association Authority to Provide Cryptocurrency Custody Services* (July 22, 2020). occ.gov

Rating vs. Assessment

GLOSSARY OF THE SETTLEMENT INTEGRITY INSTITUTE · V1.0 · GROUP III — DISTINCTIONS

DEFINITION

A **rating** is an opinion, expressed on an ordinal scale, about the relative likelihood of a future outcome — most commonly the likelihood that an obligor will pay an obligation when due. An **assessment** is a determination, against a published methodology, that a subject does or does not satisfy specified criteria as of a stated date. A rating ranks; an assessment finds.

NOTES

The distinction is established in the regulatory architecture of each. Credit ratings issued by Nationally Recognized Statistical Rating Organizations are governed by Section 15E of the Securities Exchange Act and the rules thereunder, which treat the rating as an opinion and the methodology as the institutional product; the SEC inspects NRSROs for consistent application of methodology but does not adjudicate the rating itself.[1] Conformity assessment under ISO/IEC 17065 produces a binary determination — the product, process, or service either conforms to the specification or it does not — and the certification body's standing depends on the integrity of that determination.[2] Audit opinions under PCAOB standards similarly produce a finding (unqualified, qualified, adverse, disclaimer) against published auditing standards, not a forecast.[3]

The Operational Readiness Assessment is an assessment, not a rating. *It does not predict; it determines.* It does not rank infrastructures against one another; it finds whether a particular infrastructure satisfies the criteria of Operational Suitability as of the assessment date. The output is a finding, supported by evidence, against a published methodology — recertified on a defined cycle as conditions change. The distinction matters because the questions a rating answers and the questions an assessment answers are not the same questions, and the institutional disciplines required to answer each well are different. *A rating asks how likely; an assessment asks whether.* For tokenized settlement infrastructure, where the question regulators, counterparties, and the public need answered is whether the infrastructure is suitable for use in the discharge of obligations, the assessment is the form the answer must take.

SEE ALSO

Operational Readiness Assessment · Operational Suitability · Methodology Authority · Recertification Cycle

REFERENCES

1. Securities and Exchange Commission, *Nationally Recognized Statistical Rating Organizations*, 17 C.F.R. § 240.17g-1 et seq.; Securities Exchange Act of 1934 § 15E. ecfr.gov

2. International Organization for Standardization & International Electrotechnical Commission, *ISO/IEC 17065:2012 — Conformity Assessment: Requirements for Bodies Certifying Products, Processes and Services*. iso.org

3. Public Company Accounting Oversight Board, *AS 3101: The Auditor's Report on an Audit of Financial Statements When the Auditor Expresses an Unqualified Opinion*. pcaobus.org

Standard vs. Framework

GLOSSARY OF THE SETTLEMENT INTEGRITY INSTITUTE · V1.0 · GROUP III — DISTINCTIONS

DEFINITION

A **standard** is a specification, published by an institution with the standing to publish it, that prescribes requirements against which a subject can be assessed and a determination rendered. A **framework** is an organized set of considerations, principles, or domains intended to guide analysis, planning, or judgment, but which does not by itself prescribe the criteria against which a determination is rendered. A standard produces findings; a framework produces orientation.

NOTES

Both are useful; they do different work. The NIST Cybersecurity Framework is a framework — it organizes cybersecurity considerations into functions and categories that practitioners use to structure programs, but it does not prescribe the criteria against which a cybersecurity posture is found compliant or non-compliant.[1] ISO/IEC 27001 is a standard — it prescribes requirements for an information security management system against which an organization is certified or not certified.[2] The COSO *Internal Control — Integrated Framework* is a framework — it organizes the components of internal control; the auditing standards under PCAOB and the assessment requirements under SOX 404 are the standards against which controls are evaluated.[3]

The distinction matters for the architecture of an institution. A body that publishes frameworks is in the orientation business; a body that publishes standards is in the determination business. The disciplines are different — public methodology, due process for changes, governance over interpretation, inspection of consistent application. *A framework can be adopted; a standard must be applied.* The Operational Suitability Standard is a standard. It prescribes the criteria against which the Operational Readiness Assessment renders its finding. The Trust Fabric is a framework — it organizes the domains in which Operational Suitability must be established. Both are necessary; conflating them collapses the institutional discipline that each requires.

SEE ALSO

Methodology Authority · Operational Suitability · Trust Fabric · Operational Readiness Assessment

REFERENCES

1. National Institute of Standards and Technology, *NIST Cybersecurity Framework 2.0*, NIST CSWP 29 (February 26, 2024). nist.gov

2. International Organization for Standardization & International Electrotechnical Commission, *ISO/IEC 27001:2022 — Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements*. iso.org

3. Committee of Sponsoring Organizations of the Treadway Commission, *Internal Control — Integrated Framework* (2013). coso.org

Colophon

This is the *Glossary v1.0* of the Settlement Integrity Institute, published May 12, 2026.

The doctrine the glossary expresses is the Trust Fabric Framework. The methodology against which infrastructures are assessed is the Operational Suitability Standard. The findings the Institute issues are recorded in the Registry, on a defined recertification cycle.

Comment, correction, and contribution: comments@siistandards.com.

Settlement Integrity Institute
The infrastructure of trust for tokenized value settlement.