THE TRUST FABRIC FRAMEWORK

SETTLEMENT INTEGRITY INSTITUTE

S I I

THE STANDARD FOR TOKENIZED VALUE ASSURANCE

A Meridian Standards Group Institution

Version 1.1 | April 2026

Document Information

Classification
Public

Version
1.1

Date
April 2026

Publisher
Settlement Integrity Institute

Parent Body
Meridian Standards Group

Address
2001 L Street NW, Suite 500
Washington, DC 20036

This document is published in the public interest by the Settlement Integrity Institute. The standard is free. The authority it confers is earned.

Contents

01 Foreword

02 The Assurance Gap

- 2.1 The Component Fallacy
- 2.2 The Regulatory Signal
- 2.3 The Competitive Landscape

03 The 10 Control Domains

- Domain 1: Intent Assurance
- Domain 2: Cross-Layer Dependency Assurance
- Domain 3: Continuous Reserve Integrity
- Domain 4: Oracle and External Truth Integrity
- Domain 5: Compliance-by-Design at Transfer Time
- Domain 6: Legal Finality Mapping
- Domain 7: Containment and Recovery
- Domain 8: Human Decision Security
- Domain 9: Systemic Risk Visibility
- Domain 10: Privacy-Preserving Forensics

04 The 5 Assurance Layers

- Layer 1: Asset Truth
- Layer 2: Transaction Truth
- Layer 3: Policy Truth
- Layer 4: Operational Truth
- Layer 5: Legal and Recovery Truth

05 The 7 Trust Verdicts

06 Domain-Layer-Verdict Mapping

07 Adoption and Assessment

- 7.1 Scoring Methodology
- 7.2 Intended Audience
- 7.3 Relationship to Existing Standards

08 Conclusion

Sources

01
Foreword

The financial system is undergoing its most significant structural transformation in a generation. Tokenized deposits, stablecoins, and central bank digital currencies are no longer theoretical — they are being built, regulated, and deployed at scale. SWIFT's shared ledger MVP connects tokenized deposits across 200+ countries. The US GENIUS Act imposes bank-grade compliance on stablecoin issuers. The EU's MiCA regulation is live. Central banks from Singapore to the UAE have enacted comprehensive frameworks. The infrastructure of global value settlement is being rebuilt, and the world needs it to be right.

Yet the infrastructure that assures these instruments — that verifies their integrity from human intent to legal settlement — does not exist.

The industry has built custody solutions, chain analytics platforms, compliance screening tools, and reserve attestation processes. Each addresses a component. None addresses the whole. No neutral, cross-layer, policy-aware assurance fabric validates that a tokenized transaction is what it claims to be, backed by what it claims to hold, compliant with the rules that govern it, and recoverable when it fails.

> The Trust Fabric Framework is that standard.

This specification defines 10 control domains, 5 assurance layers, and 7 trust verdicts that together constitute a complete assurance architecture for tokenized value settlement. It is designed to be adopted by stablecoin issuers, custody platforms, bridge operators, banks, regulators, and central banks as the reference standard against which transaction assurance readiness is measured.

The framework does not replace existing standards. It builds on the foundation laid by BIS/CPMI-IOSCO's Principles for Financial Market Infrastructures,[4] NIST's Web3 and stablecoin security research,[2,3] FATF's Travel Rule and virtual asset guidance,[5] the FSB's crypto-asset recommendations,[6] and the regulatory frameworks now being enacted across major jurisdictions. What it adds is the unifying assurance layer that these bodies have called for but no institution has yet defined.

> ***The Settlement Integrity Institute publishes this framework in the public interest. The standard is free. The authority it confers is earned.***

2. NIST IR 8475, "A Security Perspective on the Web3 Paradigm," April 2024 — https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8475.ipd.pdf

3. NIST IR 8408, “Understanding Stablecoin Technology and Related Security Considerations” — https://csrc.nist.gov/pubs/ir/8408/final
4. BIS/CPMI-IOSCO, “Application of the PFMI to Stablecoin Arrangements,” July 2022 — https://www.bis.org/cpmi/publ/d206.htm
5. FATF, “Recommendation 15 Implementation Review,” June 2025 — https://www.fatf-gafi.org/
6. FSB, “Thematic Peer Review on Crypto-Asset Regulation,” October 2025 — https://www.fsb.org/2025/10/fsb-finds-significant-gaps...

02

The Assurance Gap

2.1 The Component Fallacy

Every major incident in tokenized finance shares a structural characteristic: the individual components performed as designed, but the transaction as a whole was not assured.

On February 21, 2025, the Bybit exchange suffered a $1.5 billion theft — the largest in cryptocurrency history.[1] The cryptographic primitives were sound. The multisignature wallet required three authorized signers. The custody infrastructure was institutional-grade. The failure occurred in the space between what signers believed they were approving and what was actually executed. Attackers compromised the web interface of Safe{Wallet}, a third-party multisig platform, by injecting malicious JavaScript through a compromised developer machine. The code altered transaction data after display but before signing. Three authorized signers approved what appeared to be a routine internal transfer. They were, in fact, transferring control of the cold wallet's smart contract to North Korean state-sponsored actors.

> ***NCC Group's forensic analysis confirmed the attack exploited the gap between displayed intent and execution payload. The cryptography was never broken. The custody was never breached. The trust fabric between human intent and on-chain settlement simply did not exist.[1]***

This is not an isolated failure. It is a structural condition.

2.2 The Regulatory Signal

Global regulators are converging on a single conclusion: component-level security is insufficient for value infrastructure.

BIS/CPMI-IOSCO: The Principles for Financial Market Infrastructures (PFMI) establish 24 principles for systemically important payment systems. The 2022 guidance on stablecoin arrangements explicitly extends these principles to stablecoins used for payments, demanding governance, comprehensive risk management, settlement finality, and money settlement standards.[4] The guidance confirms: if a stablecoin arrangement is systemically important, it must observe all relevant PFMI principles — not selectively.

NIST: Internal Report 8475 (Web3 Security, 2024) and IR 8408 (Stablecoin Security Considerations) identify cross-layer risks, bridge vulnerabilities, oracle compromise, and immature operational patterns as foundational threats.[2,3] These are not component failures — they are fabric failures.

FATF: The 2025 review of Recommendation 15 implementation across 67 jurisdictions finds that stablecoin use by illicit actors is rising, Travel Rule implementation remains uneven globally (85% enacted or in process, significant gaps in enforcement), and cross-border transparency remains structurally inadequate.[5]

FSB: The October 2025 thematic peer review across 37 jurisdictions finds "significant gaps and inconsistencies" in crypto-asset regulation, with lending, borrowing, and margin trading often excluded from frameworks entirely. Only 11 of 19 jurisdictions with finalized frameworks have implemented comprehensive reporting.[6]

Central Bank of Ireland: Discussion Paper 12 (March 2026) on DLT and tokenisation in financial services raises unresolved risks in oracle trust, settlement finality, smart contract governance, digital identity and verification, and governance transparency — directly mirroring five of the ten control domains defined in this framework.[7]

IMF: Multiple papers identify legal certainty as a major stablecoin risk, particularly cross-border. DLT raises unresolved questions about applicable law, ownership rights, and enforceability of claims against tokenized instruments.

Bank of England: The November 2025 consultation paper on sterling-denominated systemic stablecoins proposes using PFMI as a baseline for capital requirements and explicitly addresses the absence of comprehensive failure-management regimes for stablecoin issuers.[8]

> The regulatory signal is unambiguous. The frameworks being mandated require an assurance standard that does not yet exist. The Trust Fabric Framework fills that gap.

2.3 The Competitive Landscape

The institutions building tokenized finance infrastructure are doing exactly what they were designed to do. The assurance gap is not a failure of any single platform — it is a structural consequence of a market that built its components before it built its standard.

Chainalysis and Elliptic provide chain analytics and AML screening that are essential to the compliance infrastructure of tokenized markets — delivering real coverage across Domains 5 and 10. Their work is valuable and widely adopted. What it does not address — and was never designed to address — is intent verification, reserve integrity, legal finality, containment readiness, or cross-layer dependency health. On-chain pattern analysis is one layer of a larger fabric.

Fireblocks provides custody infrastructure, MPC key management, and policy engines that underpin the operational security of tokenized asset platforms — addressing foundational elements of Domains 1 and 8. It is a vendor platform built to hold and move assets with precision. A neutral assurance layer requires independence from the infrastructure it assesses. Reserve truth, legal finality, systemic risk visibility, and oracle integrity sit outside its mandate by design.

SWIFT is building something significant: an interoperability rail for tokenized deposits connecting banks across 200+ countries, with a shared ledger MVP going live in 2026. SWIFT provides the rail.

The assurance layer — the verification that what moves across that rail is what it claims to be — remains the open question. Banks retain authority over keys, funding, and settlement decisions. The standard that governs those decisions does not yet travel with the rail.

Circle and other stablecoin issuers have advanced reserve transparency further than most of the market expected. Periodic attestations represent a genuine step toward accountability. They are, by their nature, backward-looking point-in-time snapshots. Continuous, real-time, cross-layer assurance is a different instrument entirely — and it is what the institutions now building on these rails are beginning to require.

Blockdaemon has published work on intent verification, the closest existing approach to Domain 1. It remains a single-layer solution within a broader infrastructure offering.

> The Trust Fabric Framework is not a response to any of these platforms. It is the layer that completes what all of them are pointing toward.

---

1. NCC Group, "In-Depth Technical Analysis of the Bybit Hack," March 2025 — https://www.nccgroup.com/research/in-depth-technical-analysis-of-the-bybit-hack/

7. Central Bank of Ireland, "Discussion Paper 12: DLT & Tokenisation in Financial Services," March 2026 — https://www.centralbank.ie/publication/discussion-papers/

8. Bank of England, "Proposed Regulatory Regime for Sterling-Denominated Systemic Stablecoins," Nov 2025 — https://www.bankofengland.co.uk/paper/2025/cp/proposed-regulatory-regime...

03

The 10 Control Domains

The Trust Fabric Framework defines 10 control domains. Together, they constitute the complete assurance surface for tokenized value settlement — built for the market that exists today, not the market that existed before it. Each domain identifies a specific assurance gap: a category of trust that must be continuously verified for a transaction to be considered settlement-ready.

Domain 1

Intent Assurance

What is verified: The action approved by human signers is materially identical to the action executed on-chain.

The gap: No widely deployed signing layer simulates post-transaction state, renders the economic outcome in plain language, flags abnormal privilege changes, or cryptographically binds displayed intent to execution payload.

> ***Evidence: The Bybit theft ($1.5B, February 2025) exploited precisely this gap. NCC Group's analysis confirmed: "Bybit signers blind-signed the messages without carefully checking their contents, trusting what the Safe Web3 Application displayed." The attack succeeded not because cryptography failed, but because the assurance bridge between human cognition and machine execution did not exist.***[1]

Control objectives:

- Pre-signing simulation of post-transaction state
- Plain-language rendering of economic outcome for all signers
- Anomaly detection for privilege escalation, contract modification, and destination changes
- Cryptographic binding of displayed intent to signed payload
- Independent verification channel for high-value transactions

Domain 2

Cross-Layer Dependency Assurance

What is verified: All critical dependencies — wallet, UI, identity provider, smart contract, oracle, bridge, API, off-chain service — are healthy and trustworthy at the moment of settlement.

The gap: No control plane evaluates the health and trust posture of all critical dependencies before allowing a transaction to settle. Each dependency is monitored in isolation, if at all.

> ***Evidence: NIST IR 8475 identifies cross-layer risks as a foundational Web3 security concern.[2] Bridge exploits have caused hundreds of millions in losses. The Bybit attack was a cross-layer failure: the compromise of a third-party UI provider (Safe{Wallet}) defeated the exchange's own custody controls.[1]***

Control objectives:

- Real-time health assessment of all transaction-critical dependencies
- Dependency trust scoring with configurable thresholds
- Automatic degradation or halt when dependency trust falls below threshold
- Supply chain mapping for all third-party components in the transaction path
- Continuous monitoring of bridge, oracle, and API availability and integrity

Domain 3

Continuous Reserve Integrity

What is verified: The token in transit is fully backed, redeemable, and unencumbered at the moment of settlement — not as of the last quarterly attestation.

The gap: Current reserve assurance is periodic, backward-looking, and issuer-controlled. Attestations are point-in-time snapshots that do not reflect intraday redemption pressure, real-time liability matching, or operational redemption capacity.

> ***Evidence: NIST IR 8408 identifies reserve design and trust assumptions as foundational stablecoin security considerations.[3] The Bank of England's 2025 consultation proposes specific reserve composition requirements (minimum 40% central bank deposits) precisely because existing attestation practices are insufficient.[8] MiCA imposes reserve segregation and composition requirements for the same reason.***

Control objectives:

- Live, tamper-evident reserve proofs tied to outstanding token supply
- Real-time liability matching between issued tokens and backing assets
- Operational redemption capacity verification (not just reserve existence)
- Independent reserve verification by credentialed third parties
- Automatic alerting when reserve ratios breach configurable thresholds

Domain 4

Oracle and External Truth Integrity

What is verified: External data feeds (price, identity, compliance, reference data) entering the transaction are accurate, timely, and have not been compromised.

The gap: Oracle systems are trusted implicitly. No widely deployed standard requires multi-source quorum validation for external truth or automatic throttling when feeds diverge.

> ***Evidence: NIST IR 8475 identifies oracle compromise as a primary attack vector.[2] Central Bank of Ireland DP12 explicitly raises oracle trust as an unresolved risk for tokenised financial services.[7] Oracle manipulation has been a recurring vector in DeFi exploits, with losses exceeding $1 billion cumulatively.***

Control objectives:

- Multi-source quorum validation for all external data feeds
- Divergence detection with automatic throttling or safe-mode activation
- Staleness detection and freshness enforcement for time-sensitive data
- Tamper-evident provenance chain for all oracle inputs
- Independent oracle health scoring visible to transaction participants

Domain 5

Compliance-by-Design at Transfer Time

What is verified: The transfer is compliant with all applicable sanctions, AML/CFT, jurisdiction, identity, and transfer constraints at the moment of execution — not retroactively.

The gap: Compliance is predominantly applied after the fact. Stablecoin transfers settle first and are screened later. The Travel Rule remains unevenly implemented globally. No standard exists for policy-aware money that enforces jurisdiction-specific constraints at execution time without destroying privacy or interoperability.

> ***Evidence: FATF's 2025 review finds stablecoin use by illicit actors rising, Travel Rule implementation at 85% enacted or in process but with significant enforcement gaps, and cross-border transparency structurally inadequate.[5] The report highlights that information binding — connecting identity data to the payment itself — remains an unsolved challenge across most implementations.***

Control objectives:

- Real-time sanctions screening at transfer initiation
- Jurisdiction-aware policy enforcement embedded in transaction flow
- Travel Rule compliance with cryptographic identity binding
- Privacy-preserving compliance verification (selective disclosure)
- Configurable transfer constraints (amount limits, velocity limits, counterparty restrictions)

Domain 6

Legal Finality Mapping

What is verified: The transaction maps to a defined legal outcome — who owns what, under which jurisdiction's law, with what rights of dispute, freeze, redemption, and insolvency treatment.

The gap: Tokenized transactions execute in code. Legal systems operate in text. No machine-readable legal overlay maps wallet actions, token claims, freeze/redemption rights, insolvency treatment, and dispute mechanisms to legal entities and jurisdictions.

> ***Evidence: The IMF has published multiple papers identifying legal certainty as a major stablecoin risk, especially cross-border. DLT raises unresolved questions about applicable law, ownership, and enforceability. BIS/CPMI-IOSCO PFMI guidance demands settlement finality[4] — a legal concept that has no standardized mapping to on-chain settlement.***

Control objectives:

- Machine-readable legal overlay for all tokenized instruments
- Jurisdiction mapping for each party and each asset in the transaction
- Defined dispute resolution, freeze, and redemption mechanisms
- Insolvency treatment mapping (What happens if the issuer fails?)
- Legal finality attestation — confirmation that on-chain settlement constitutes settlement at law

Domain 7

Containment and Recovery

What is verified: If the transaction fails, is compromised, or triggers a systemic event, defined containment and recovery mechanisms exist and are operational.

The gap: No interoperable containment standard exists for tokenized finance. Transaction quarantine, confidence-tiered settlement, segmented liquidity, emergency pause, and coordinated incident signaling are implemented ad hoc by individual platforms, if at all.

> ***Evidence: NIST IR 8475 identifies ecosystem-level recovery gaps as a foundational Web3 concern.[2] The FSB's 2025 review finds that most jurisdictions lack comprehensive frameworks for managing the failure of crypto-asset service providers.[6] The Bank of England's 2025 consultation explicitly addresses the absence of resolution regimes comparable to banking (FSCS, resolution tools) for stablecoin issuers.[8]***

Control objectives:

- Transaction quarantine capability for suspicious or anomalous transactions
- Confidence-tiered settlement (immediate / delayed / held-for-review)
- Segmented liquidity pools to prevent contagion across instruments
- Emergency pause capability with defined activation criteria and governance
- Coordinated incident signaling across platforms and jurisdictions

- Defined recovery and remediation procedures for each failure mode

Domain 8

Human Decision Security

What is verified: The humans in the approval workflow are operating within cognitive safety margins, with appropriate role separation, out-of-band confirmation, and decision-support infrastructure.

The gap: Operator-centric safeguards for tokenized value infrastructure are almost entirely absent. Approval workflows lack cognitive load assessment, role separation is inconsistent, out-of-band confirmation is rare, and human-risk scoring does not exist.

> ***Evidence:** The Bybit attack succeeded because three authorized signers approved a malicious transaction — not because they were negligent, but because the system was designed in a way that made human verification practically impossible. NCC Group noted: "the human factor should be taken into account in threat modeling, as blind signing is highly likely to occur."[1] The 2025 infrastructure attack trend confirms that the human decision layer is the primary target.*

Control objectives:

- Cognitive load assessment for high-value approval workflows
- Mandatory role separation for transaction initiation, approval, and execution
- Out-of-band confirmation for transactions exceeding defined thresholds
- Human-risk scoring (fatigue, time pressure, anomalous behavior patterns)
- Decision-support dashboards that surface material risk factors before signing
- Cooling-off periods for irreversible, high-value transactions

Domain 9

Systemic Risk Visibility

What is verified: Banks, issuers, regulators, and systemic risk monitors have visibility into concentration risk, dependency failure chains, liquidity stress, and cross-platform contagion potential.

The gap: No shared assurance mesh gives institutional participants visibility into systemic risk across tokenized financial infrastructure. Each platform operates as an island. Concentration risk, dependency chains, and contagion pathways are invisible.

> ***Evidence:** The FSB's 2025 thematic review identifies the lack of comprehensive reporting as a critical gap — only 11 of 19 jurisdictions with finalized frameworks have reporting requirements in place.[6] The FSB notes: "uneven implementation creates opportunities for regulatory arbitrage and complicates oversight of the inherently global and evolving crypto-asset market."*

Control objectives:

- Concentration risk monitoring across issuers, custodians, and platforms
- Dependency failure chain mapping (what breaks if X fails?)
- Liquidity stress indicators visible to authorized institutional participants
- Cross-platform contagion modeling
- Standardized systemic risk reporting format for regulatory consumption
- Real-time risk dashboards for systemic risk monitors

Domain 10

Privacy-Preserving Forensics

What is verified: Authorized parties can verify identity, compliance, reserve claims, and transaction integrity without exposing unnecessary data to unauthorized parties.

The gap: The tension between enforcement visibility and legitimate privacy remains unresolved. Full transparency destroys commercial confidentiality. Full privacy prevents compliance. No selective-disclosure evidence system exists that balances both requirements for tokenized value infrastructure.

> ***Evidence: FATF explicitly acknowledges the tension between enforcement visibility and legitimate privacy in its Travel Rule guidance.[5] MiCA's privacy requirements and GDPR create compliance obligations that conflict with full on-chain transparency. The Central Bank of Ireland's DP12 identifies digital identity and verification as a critical enabler that remains inadequately addressed.[7]***

Control objectives:

- Selective-disclosure proofs for identity verification
- Zero-knowledge or minimal-disclosure compliance attestations
- Cryptographic evidence preservation for forensic investigation
- Graduated access controls (regulator, auditor, counterparty, public)
- Privacy-preserving audit trail that satisfies both enforcement and confidentiality requirements

04

The 5 Assurance Layers

The 10 control domains describe what must be verified. The 5 assurance layers describe what categories of truth must be established for a transaction to be settlement-ready. Each layer represents a distinct dimension of assurance that cannot be reduced to or substituted by another.

Layer 1

Asset Truth

Proves: What the token is, what backs it, who can redeem it, where reserves sit, and what legal rights attach.

This layer establishes the foundational truth about the instrument itself. A token that claims to be worth one dollar must be verifiably backed by assets worth one dollar, redeemable under defined conditions, and subject to identifiable legal rights. Asset Truth draws primarily on Domain 3 (Continuous Reserve Integrity) and Domain 6 (Legal Finality Mapping).

Key sources: NIST IR 8408,[3] IMF stablecoin legal/operational risk papers, Bank of England systemic stablecoin consultation.[8]

Layer 2

Transaction Truth

Proves: What the user intended, what was signed, what dependencies were involved, and what the expected post-state should be.

This layer establishes that the transaction is what it appears to be — that intention, signature, execution, and outcome are aligned. Transaction Truth draws primarily on Domain 1 (Intent Assurance) and Domain 2 (Cross-Layer Dependency Assurance).

Key sources: NCC Group Bybit analysis,[1] NIST IR 8475.[2]

Layer 3

Policy Truth

Proves: The transfer was compliant with all applicable sanctions, AML/CFT, jurisdiction, travel rule, and transfer constraints at the moment of execution.

This layer establishes that the transaction is lawful. Policy Truth draws primarily on Domain 5 (Compliance-by-Design) and Domain 10 (Privacy-Preserving Forensics).

Key sources: FATF 2025 Recommendation 15 review,[5] MiCA, US GENIUS Act, UK FCA authorization requirements.

Layer 4

Operational Truth

Proves: Custody workflow, key access, bridge state, oracle health, admin actions, and segregation-of-duties are all within tolerance at the moment of settlement.

This layer establishes that the operational infrastructure supporting the transaction is healthy and properly governed. Operational Truth draws primarily on Domain 2 (Cross-Layer Dependency Assurance), Domain 4 (Oracle and External Truth Integrity), and Domain 8 (Human Decision Security).

Key sources: NIST IR 8475,[2] Central Bank of Ireland DP12,[7] 2025 infrastructure attack patterns.

Layer 5

Legal and Recovery Truth

Proves: What happens if the transaction is disputed, frozen, reversed, redeemed, or subject to insolvency, sanctions, or regulatory intervention.

This layer establishes that the consequences of failure are defined and manageable. Legal and Recovery Truth draws primarily on Domain 6 (Legal Finality Mapping) and Domain 7 (Containment and Recovery).

Key sources: IMF papers, BIS/CPMI-IOSCO PFMI guidance,[4] FSB 2025 thematic review,[6] Bank of England 2025 consultation.[8]

05

The 7 Trust Verdicts

Before a tokenized transaction is permitted to settle, the Trust Fabric produces a composite trust verdict across seven dimensions. Each verdict is a binary or graduated assessment. If any verdict fails, the transaction does not proceed to full settlement — it degrades safely.

Verdict 1: Identity

Do we know which legal or institutional actor is behind this action? Is the identity verified, current, and sufficient for the jurisdictional requirements of this transaction?

Verdict 2: Intent

Is the approved action materially the same as the executed action? Has the signer seen an accurate representation of the post-transaction state?

Verdict 3: Asset Quality

Is the token fully backed, redeemable, and unencumbered right now — not as of the last attestation, but at the moment of settlement?

Verdict 4: Dependency Health

Are the bridge, oracle, smart contract, custody, and other dependencies behaving normally? Is any critical dependency degraded, compromised, or unavailable?

Verdict 5: Policy Compliance

Can this transfer lawfully occur under the relevant rules of every jurisdiction it touches?

Verdict 6: Operational Integrity

Did the workflow meet separation-of-duty standards, approval thresholds, and operational safeguards?

Verdict 7: Recovery Posture

If this transaction goes wrong, is there a defined containment and remedy path? Are quarantine, rollback, dispute, and recovery mechanisms operational?

Degradation Model

Not every failed verdict results in denial. The Trust Fabric employs graduated degradation:

- All verdicts pass → Full-speed settlement
- Non-critical verdict degraded → Delayed settlement with enhanced monitoring
- Critical verdict degraded → Held settlement requiring additional authorization
- Multiple verdicts failed → Quarantined transaction with incident escalation
- Systemic indicators triggered → Emergency pause with coordinated signaling

This graduated approach reflects what the market actually needs: an assurance layer that protects integrity without becoming an obstacle to legitimate commerce. The goal is not to stop transactions — it is to ensure the ones that proceed are transactions the market can trust. It mirrors the risk-based approach that regulators universally advocate and that the market has always deserved.

06

Domain-Layer-Verdict Mapping

The following table maps each control domain to its primary assurance layers and trust verdicts, illustrating how the three dimensions of the framework interconnect.

Domain	Primary Layer(s)	Primary Verdict(s)
1. Intent Assurance	Transaction Truth	Intent
2. Cross-Layer Dependency	Transaction Truth, Operational Truth	Dependency Health
3. Continuous Reserve Integrity	Asset Truth	Asset Quality
4. Oracle & External Truth	Operational Truth	Dependency Health
5. Compliance-by-Design	Policy Truth	Policy Compliance
6. Legal Finality Mapping	Asset Truth, Legal & Recovery Truth	Identity, Recovery Posture
7. Containment & Recovery	Legal & Recovery Truth	Recovery Posture
8. Human Decision Security	Operational Truth	Operational Integrity
9. Systemic Risk Visibility	All Layers	All Verdicts (systemic overlay)
10. Privacy-Preserving Forensics	Policy Truth	Identity, Policy Compliance

Domain 9 (Systemic Risk Visibility) functions as a systemic overlay, drawing on signals from all five assurance layers and informing all seven trust verdicts. It does not produce an independent verdict but modulates the confidence and urgency applied to every other verdict.

07

Adoption and Assessment

7.1 Scoring Methodology

The Settlement Integrity Institute publishes a companion document — the SII Transaction Assurance Readiness Score (SII-TARS) — defining the methodology for assessing organizations against the 10 control domains. The assessment follows a domain-by-domain structure with weighted scoring, maturity levels, and actionable gap analysis. The result is a dated, versioned verdict that gives the market a reference it can rely on.

7.2 Intended Audience

- Stablecoin issuers seeking to demonstrate assurance readiness
- Custody platforms and wallet providers building transaction infrastructure
- Bridge operators connecting tokenized ecosystems
- Banks integrating tokenized deposits into existing settlement systems
- Securities exchanges exploring tokenized instrument listing and assurance
- Asset managers seeking assurance standards for tokenized portfolios
- Regulators developing supervisory frameworks for tokenized finance
- Central banks designing CBDC assurance architectures
- Insurance underwriters pricing risk for tokenized financial infrastructure
- Auditors and assessors evaluating transaction assurance posture

7.3 Relationship to Existing Standards

The Trust Fabric Framework was built to work alongside the standards that already govern global financial infrastructure — not to replace them. The bodies that defined those standards identified the assurance gap this framework fills. The TFF operationalizes their mandates:

- BIS/CPMI-IOSCO PFMI: The Trust Fabric operationalizes PFMI principles for tokenized settlement[4]
- NIST: The framework addresses the security considerations identified in IR 8475 and IR 8408[2,3]
- FATF: Domains 5 and 10 operationalize Travel Rule and AML/CFT requirements[5]

- MiCA / GENIUS Act / FCA: The framework provides an assessment structure for regulatory compliance
- ISO 20022: Policy Truth layer aligns with structured messaging standards for financial transactions

08

Conclusion

The world's value infrastructure is being rebuilt on programmable rails. The instruments are new. The risks are not.

Every financial crisis in history shares a common architecture: components that worked individually but failed collectively. The Trust Fabric Framework exists to ensure that tokenized value is not the next chapter in that pattern.

> Ten domains. Five layers. Seven verdicts. One standard.

The standard is published. The meridian is set.

Settlement Integrity Institute
A Meridian Standards Group Body
April 2026

Sources

1. NCC Group, “In-Depth Technical Analysis of the Bybit Hack,” March 2025
https://www.nccgroup.com/research/in-depth-technical-analysis-of-the-bybit-hack/

2. NIST IR 8475, “A Security Perspective on the Web3 Paradigm,” April 2024
https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8475.ipd.pdf

3. NIST IR 8408, “Understanding Stablecoin Technology and Related Security Considerations”
https://csrc.nist.gov/pubs/ir/8408/final

4. BIS/CPMI-IOSCO, “Application of the PFMI to Stablecoin Arrangements,” July 2022
https://www.bis.org/cpmi/publ/d206.htm

5. FATF, “Recommendation 15 Implementation Review,” June 2025
https://www.fatf-gafi.org/

6. FSB, “Thematic Peer Review on Crypto-Asset Regulation,” October 2025
https://www.fsb.org/2025/10/fsb-finds-significant-gaps-and-inconsistencies-in-implementation-of-crypto-and-stablecoin-recommendations/

7. Central Bank of Ireland, “Discussion Paper 12: DLT & Tokenisation in Financial Services,” March 2026
https://www.centralbank.ie/publication/discussion-papers/

8. Bank of England, “Proposed Regulatory Regime for Sterling-Denominated Systemic Stablecoins,” November 2025
https://www.bankofengland.co.uk/paper/2025/cp/proposed-regulatory-regime-for-sterling-denominated-systemic-stablecoins