Bitcoin Custody Standard (BCS)

Public Normative Summary
Document ID: BCS-NS-1.0
Version: 1.0
Status: Public, Citable
Publication Date: February 2026
Next Scheduled Review: February 2027 (or earlier if major revision required)

Abstract. The Bitcoin Custody Standard (BCS) establishes a normative framework for evaluating and strengthening the resilience of Bitcoin custody architectures against Custodial Entropy over time. The Bitcoin Custody Resilience Index (BCRI) is the quantitative assessment instrument aligned with BCS, providing structured scoring across the five structural pillars. BCRI incorporates three headline metrics:

- Bitcoin Custody Resilience Index (BCRI): Structural resilience (0-100, higher is stronger)
- Entropy Risk Index (ERI): Time-based structural fragility (0-100, lower is better)
- Exposure Risk Index (XRI): Adversarial and visibility risk (0-100, lower is better)

BCS is designed to operate alongside evolving institutional, regulatory, and technological custody frameworks while remaining structurally independent of jurisdiction-specific requirements.

1. Purpose

The Bitcoin Custody Standard (BCS) establishes a normative framework for evaluating and strengthening the resilience of Bitcoin custody architectures against Custodial Entropy over time.

Custodial Entropy is the inevitable structural degradation of custody systems over time due to forgotten knowledge, undocumented changes, technological evolution, shifting life circumstances, coordination complexity, and insufficient review.

Because Bitcoin is a bearer asset with no recovery possible once keys are lost, BCS exists to reduce the probability that Bitcoin holdings (whether managed by individuals, families, fiduciaries, advisors, or institutions) become permanently inaccessible due to preventable Custodial Entropy.

Bitcoin was introduced as a peer-to-peer electronic cash system in which ownership is defined exclusively by control of private keys, without reliance on centralized recovery authorities (Nakamoto, 2008). BCS operates within this foundational architectural constraint.

BCS defines standardized terminology, structural domains, and conformance requirements to support consistent evaluation and long-term preservation of access across custody contexts.

The Bitcoin Custody Resilience Index (BCRI) is the quantitative assessment instrument aligned with BCS. BCRI provides structured measurement and reporting across the five BCS structural pillars, including assessment of Entropy Risk through a proprietary Entropy Index.

[1] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf

BCS defines the normative framework; BCRI operationalizes that framework through structured scoring and reporting.

2. Scope

BCS applies to Bitcoin private-key custody architectures, including but not limited to:
- Single-signature cold storage
- Self-managed multi-signature custody
- Collaborative or assisted multi-signature custody
- Hot or online wallet architectures (where applicable)

BCS evaluates custody resilience only. BCS does not evaluate price risk, trading strategy, portfolio allocation, tax treatment, or investment suitability.

3. Definitions

Assurance Tier: The level of conformance claim: Self-Assessment (user-declared), Verified (second-party evidence review), or Independent Certification (third-party).
Bitcoin Custody Resilience Index (BCRI): A composite structural resilience score (0-100) derived from weighted scoring across the five BCS structural pillars. Higher values indicate stronger structural resilience.
Continuity Risk: The risk that Bitcoin becomes inaccessible due to death, incapacity, or unclear succession planning.
Conformance: A documented determination that a custody architecture satisfies BCS requirements at a stated Assurance Tier, referencing the applicable BCS version.
Coordination Risk: The risk that recovery or signing fails because excessive participant steps, dependencies, or sequencing requirements are required for system operation.
Coercion Risk: The risk that access is compromised under physical, legal, or social pressure.
Custodial Entropy: The progressive degradation of a custody system over time resulting from knowledge loss, technological evolution, undocumented modifications, environmental change, coordination breakdown, or insufficient review.
Custody Architecture: The structured design describing how private keys, recovery material, participants, devices, documentation, and recovery procedures are organized to preserve control over Bitcoin across time.
Custody Resilience: The degree to which a custody architecture remains secure, recoverable, and operational under time, stress, and succession scenarios.
Entropy Index: A proprietary quantitative metric within the Bitcoin Custody Resilience Index (BCRI) that measures the strength of structural mitigation controls against long-horizon Custodial Entropy. The Entropy Index is scored on a 0–100 scale, where higher values indicate stronger mitigation of entropy-related degradation.
Entropy Risk Index (ERI): The residual exposure to Custodial Entropy expressed on a 0-100 scale. ERI is calculated as:

$$ERI = 100 - Entropy\ Index$$

(Higher values indicate greater structural vulnerability to long-horizon degradation.)

Exposure Risk Index (XRI): An advisory measurement reflecting real-world and on-chain visibility exposure, including identity linkage, disclosure scope, lifestyle signaling, signing discipline (including transaction verification practices designed to mitigate deception risks), and

coercion preparedness (e.g., documented contingency planning for duress scenarios). XRI is scored on a 0–100 scale where lower values indicate reduced targetability and stronger operational discretion, including periodic monitoring for unintended information leakage. XRI does not form part of core structural conformance requirements.
Human Failure Probability: The likelihood of loss arising from misunderstanding, memory limitation, procedural ambiguity, miscommunication, or operational error.
Pillar (Structural Domain): A defined category of custody risk used by BCS to organize normative requirements. Pillars form the structural basis of BCRI scoring.
Recovery Material: Any artifact, information, or configuration data required to authorize or restore control over Bitcoin funds, including seed phrases, private keys, passphrases, wallet descriptors, derivation paths, xpubs, and multi-signature configuration data.
Single Point of Failure: Any single missing element or event that can cause catastrophic compromise or permanent loss of access.
Standard Versioning: All conformance claims shall reference the BCS version used for assessment and shall not imply applicability to future versions without reassessment.

4. Structural Pillars

1. Cryptographic Integrity: Requirements relating to secure key generation, disciplined handling of private key material, preservation of cryptographic configuration data, and awareness of long-horizon algorithmic resilience planning.
2. Physical Distribution: Requirements relating to redundancy and separation of recovery material across independent physical risk domains, eliminating single physical points of failure.
3. Cognitive Reliability: Requirements ensuring custody and recovery do not depend on fragile memory or undocumented knowledge. Recovery procedures shall be documented and reproducible.
4. Operational & Dependency Risk: Requirements addressing reliance on tools, vendors, devices, cosigners, and coordination processes. Material dependencies shall be identified and supported by contingency pathways.
5. Temporal Resilience: Requirements ensuring long-horizon survivability, including documented review cadence, recovery validation, succession planning, change control, and mitigation of Custodial Entropy.

4.1 Multi-Metric Resilience Model

BCS evaluates custody resilience across three independent but interacting dimensions:
1. Structural Resilience (BCRI): evaluates architecture strength across defined structural pillars.
2. Temporal Fragility (ERI): represents the residual structural vulnerability to long-horizon degradation after entropy mitigation controls are applied.
3. Exposure Risk (XRI): evaluates adversarial visibility and operational security posture.

BCRI and ERI are normative structural measurements.
XRI is advisory and does not independently determine conformance status.

This separation ensures that structural resilience, time-based durability, and adversarial exposure are assessed without conflating their respective risk domains.

5. High-Level Conformance Requirements

A custody architecture claiming BCS conformance:

- Shall document its custody architecture classification and recovery dependencies.
- Shall maintain documented recovery pathways identifying required recovery material and participant thresholds.
- Shall maintain documented continuity provisions addressing incapacity and death.
- Shall maintain a defined review cadence intended to mitigate Custodial Entropy.
- Shall identify material operational dependencies and define contingency pathways.
- Shall disclose the applicable Assurance Tier under which the conformance claim is made.
- Shall reference the specific BCS version used for assessment.

5.1 Assurance Tiers

BCS recognizes three Assurance Tiers:

- Self-Assessment (first-party, user-declared).
- Verified (second-party evidence review conducted by the BCS scheme owner or designated reviewer).
- Independent Certification (third-party conformity assessment conducted by an entity independent of both the assessed party and the BCS scheme owner).

Self-Assessment:

Self-Assessment consists of structured self-evaluation against published BCS criteria and BCRI scoring methodology. Self-Assessment is valid only when performed honestly and without material omission. No independence or third-party review is implied.

Verified (Second-Party)

Verified conformance involves documented evidence review conducted by the BCS scheme owner or an authorized second-party reviewer.
Verification may include review of:

- Architectural documentation
- Recovery runbooks (non-sensitive excerpts)
- Dependency disclosures
- Review cadence documentation
- Signed attestation

Verification does not require disclosure of private keys or sensitive recovery material. Verified conformance does not constitute independent certification.

Independent Certification (Third-Party)

Independent Certification involves formal third-party conformity assessment conducted by an entity that is operationally and financially independent of both the custody architecture operator and the BCS scheme owner. Independent Certification is not implied unless explicitly stated. No claim of Independent Certification shall be made without formal third-party designation.

5.2 Conformance Limitations

BCS conformance reflects fulfillment of defined structural requirements at a stated Assurance Tier. It does not constitute a guarantee of security, protection from loss, or immunity from compromise.

5.3 Certification Threshold Logic

Unless otherwise specified:
• BCRI shall meet or exceed the defined minimum resilience threshold.
• ERI shall not exceed the defined maximum entropy risk threshold.
• XRI shall be reported but shall not independently disqualify conformance.

Threshold values may vary by architecture class and Assurance Tier and shall be published in the applicable BCRI scoring documentation. Interpretation bands for BCRI, ERI, and XRI are defined in the BCRI scoring documentation and are intended to provide structured improvement guidance.

6. Proprietary Boundary Notice

The Entropy Index, Entropy Risk Index (ERI), and Exposure Risk Index (XRI) are proprietary measurement constructs within the BCRI tool and are not themselves standalone normative requirements under BCS.