Bitcoin Custody Standard (BCS)

Public Normative Summary
Document ID: BCS-NS-1.1
Version: 1.1
Document Class: Normative Framework
Status: Public, Citable
Publication Date: March 2026
Next Scheduled Review: February 2027 (or earlier if major revision required)
Steward: Bitcoin Custody Standard Initiative

Revision History

- **Version: 1**
  - **Date:** February 2026
  - **Description:** Initial public release of the Bitcoin Custody Standard Normative Summary.
- **Version: 1.1**
  - **Date:** March 2026
  - **Description:** Clarified relationship between BCS and the BCRI assessment methodology, refined Custodial Entropy terminology, and updated conformance language.

Abstract. The Bitcoin Custody Standard (BCS) defines a normative framework for evaluating the structural resilience of Bitcoin custody architectures across time. The Bitcoin Custody Resilience Index (BCRI) is the quantitative assessment methodology aligned with BCS and used to measure custody resilience under the standard. The framework evaluates custody architectures across the five BCS structural pillars through the Architecture Resilience Score (ARS) while also assessing coordination health (CHS) , entropy-related degradation (ERI) , and adversarial exposure conditions (XRI). BCS is designed to operate alongside evolving institutional, regulatory, and technological custody frameworks while remaining structurally independent of jurisdiction-specific requirements and legal regimes.

1. Purpose

The Bitcoin Custody Standard (BCS) defines a normative framework for evaluating and strengthening the structural resilience of Bitcoin custody architectures across time. Custodial Entropy refers to the progressive structural degradation of custody systems as operational coherence erodes through knowledge loss, undocumented changes, technological evolution, coordination drift, 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. BCS operates within Bitcoin's foundational constraint that ownership is defined by control of private keys.

The Bitcoin Custody Resilience Index (BCRI) operationalizes the BCS framework by providing structured measurement of architecture resilience, coordination reliability, entropy-related degradation, and adversarial exposure.

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
- Hosted/Institutional 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. Normative References

The following document provides foundational context for the custody model addressed by this standard.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.*

4. Normative Language

The terms "shall", "should", and "may" in this document are used in accordance with standard technical specification conventions. "Shall" indicates a mandatory requirement, "should" indicates a recommended practice, and "may" indicates an optional capability.

5. Informative References

The following documents describe widely adopted technical standards and foundational research relevant to cryptographic key management and Bitcoin wallet architecture. These references are provided for contextual understanding and do not constitute requirements of the Bitcoin Custody Standard.

Bitcoin Improvement Proposals

BIP-32 *Hierarchical Deterministic Wallets.* Pieter Wuille (2012).

BIP-39 *Mnemonic Code for Generating Deterministic Keys.* Marek Palatinus, Pavol Rusnak, Aaron Voisine, Sean Bowe (2013).

BIP-174 *Partially Signed Bitcoin Transactions (PSBT).* Andrew Chow, Christopher Allen, Pieter Wuille (2017).

Cryptographic Key Management

NIST SP 800-57 *Recommendation for Key Management.* National Institute of Standards and Technology (NIST).

6. Definitions

For the purposes of this document, the following terms and definitions apply.

Architecture Resilience Score (ARS): A structural measurement of custody architecture strength derived from evaluation across the five BCS structural pillars. ARS reflects the integrity of cryptographic, physical, operational, cognitive, and temporal controls supporting custody execution. ARS is expressed on a 0–100 scale, where higher values indicate stronger architectural resilience.

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): The composite resilience output of the BCRI assessment framework integrating architecture resilience (ARS), coordination reliability (CHS), entropy-related degradation (ERI), and

adversarial exposure (XRI) into a bounded 0–100 score. Higher values indicate stronger overall custody resilience.

Composite Resilience Score (CRS): The intermediate composite resilience value produced by aggregation of effective architecture resilience (EAR) and exposure resilience (XRS) within the BCRI assessment methodology. CRS represents the preliminary structural resilience outcome prior to application of coordination adjustment and final model transformations used to derive the bounded Bitcoin Custody Resilience Index (BCRI).

Conformance: A documented determination that a custody architecture satisfies BCS requirements at a stated Assurance Tier, referencing the applicable BCS version.

Continuity Risk: The risk that Bitcoin becomes inaccessible due to death, incapacity, or unclear succession planning.

Coercion Risk: The risk that access is compromised under physical, legal, or social pressure.

Coordination Entropy Index (CEI): A measurement of structural fragility introduced by multi-party custody execution, including participant coordination requirements, governance complexity, jurisdictional dispersion, and dependencies on external actors.

Coordination Health Score (CHS): A measurement of the reliability and durability of coordination required to execute custody operations and recovery procedures. CHS reflects the stability of human participation, procedural clarity, and continuity mechanisms supporting successful custody execution across time. CHS is expressed on a 0–100 scale, where higher values indicate stronger coordination reliability.

Coordination Risk: The risk that recovery or signing fails because excessive participant steps, dependencies, or sequencing requirements are required for system operation.

Custodial Entropy: The progressive structural degradation of a Bitcoin custody architecture across time arising from two independent channels: latent operational drift and coordination fragility introduced by multi-party execution.

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 ability of a Bitcoin custody system to maintain secure, recoverable, and continuous control of private keys across time under operational, human, environmental, and adversarial stress.

Effective Architecture Resilience (EAR): Entropy-attenuated Architecture Resilience Score representing the effective structural resilience of a custody architecture after accounting for entropy-related degradation. EAR is derived from the Architecture Resilience Score (ARS) through the entropy model implemented within the BCRI assessment methodology.

Entropy Model: The analytical framework used by BCRI to measure Custodial Entropy through the Latent Entropy Index (LEI) and Coordination Entropy Index (CEI).

Entropy Resilience Score (ERS): Complementary representation of entropy resilience defined as ERS = 100 − ERI. ERS may be used for interpretive display within BCRI assessment modules but does not replace ERI as the primary entropy risk indicator.

Entropy Risk Index (ERI): A composite measurement representing the residual exposure of a custody architecture to long-horizon Custodial Entropy. ERI reflects structural vulnerability arising from both latent operational drift and coordination complexity and is expressed on a 0–100 scale, where higher values indicate greater entropy-related degradation risk.

Exposure Resilience Score (XRS): Complementary representation of exposure resilience defined as XRS = 100 − XRI, where higher values indicate lower adversarial exposure and stronger operational exposure resilience. XRS may be used for interpretive display or weighting within BCRI calculations but does not replace XRI as the primary exposure risk indicator.

Exposure Risk Index (XRI): A measurement of adversarial exposure and operational visibility conditions affecting the custody system, including identity linkage, disclosure scope, lifestyle signaling, signing discipline, and coercion preparedness. XRI is scored on a 0–100 scale where lower values indicate reduced targetability and stronger operational discretion. XRI does not independently determine conformance status but contributes to the overall resilience assessment within the BCRI framework.

Exposure Surface: The observable or inferable operational conditions through which a custody architecture may become identifiable, targetable, or vulnerable to adversarial pressure. Exposure surface includes factors such as identity linkage, disclosure practices, operational visibility, geographic concentration, signing behavior, and social or legal coercion vectors.

Human Failure Probability: The probability that loss arises from misunderstanding, memory limitations, procedural ambiguity, miscommunication, or operational error.

Latent Entropy Index (LEI): A measurement of structural degradation risk arising from internal operational drift within a custody architecture, including knowledge loss, documentation decay, technological evolution, and operational drift across time.

Pillar (Structural Domain): A defined category of custody architecture integrity 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: Conformance claims shall reference the BCS version used for assessment and shall not imply applicability to future versions without reassessment.

7. Principles of Custody Resilience

The Bitcoin Custody Standard is guided by the following principles:

• **Bearer Asset Finality.** Bitcoin ownership is defined solely by control of private keys. Loss of key material results in irreversible loss of access.

• **Structural Integrity Over Time.** Custody architectures must remain functional across long time horizons despite technological evolution, operational drift, and changing life circumstances.

• **Coordination Reliability.** Successful custody execution depends not only on cryptographic design but also on the ability of participants to coordinate signing and recovery procedures reliably.

• **Defense Against Adversarial Pressure.** Custody systems operate within adversarial environments where visibility, incentives, and coercion risks may influence system resilience.

• **Continuous Review and Adaptation.** Custody architectures require periodic review and validation to mitigate Custodial Entropy and ensure continued operational viability.

8. Structural Pillars

BCS evaluates custody resilience across five orthogonal structural domains reflecting the cryptographic, physical, operational, cognitive, and temporal conditions required to preserve control of Bitcoin across time. These pillars are intentionally designed to be analytically independent so that weaknesses within one domain cannot be obscured by strength in another.

- **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.
- **Physical Distribution:** Requirements relating to redundancy and separation of recovery material across independent physical risk domains, eliminating single physical points of failure where feasible.
- **Operational Dependency:** Requirements addressing reliance on operational tools, devices, cosigners, software, external service providers, and coordination dependencies involved in custody execution.
- **Cognitive Reliability:** Requirements ensuring custody and recovery do not depend on fragile memory or undocumented knowledge. Recovery procedures shall be documented and reproducible.
- **Temporal Resilience:** Requirements ensuring long-horizon survivability, including documented review cadence, recovery validation, succession planning, change control, and mitigation of Custodial Entropy.

8.1 Multi-Metric Resilience Model

BCS evaluates custody resilience through four interacting analytical dimensions that together determine the structural durability of a custody architecture across time.

1. **Architecture Resilience (ARS).** Evaluates the structural strength of the custody architecture across the five BCS structural pillars.

2. **Coordination Health (CHS).** Evaluates the reliability of human coordination and procedural continuity required for successful custody execution and recovery.

3. **Entropy Resilience (ERS).** Evaluates the ability of the custody architecture to resist long-horizon degradation arising from Custodial Entropy. Entropy resilience is derived from the Entropy Risk Index (ERI), which measures structural vulnerability to time-based operational drift and coordination fragility.

4. **Exposure Resilience (XRS).** Evaluates the degree to which the custody architecture minimizes adversarial exposure surface conditions that may increase targetability. Exposure resilience is derived from the Exposure Risk Index (XRI), which measures operational visibility, disclosure patterns, and coercion exposure.

ERI and XRI remain the primary risk indicators used for conformance evaluation, while ERS and XRS represent complementary resilience interpretations derived from those indices. ARS and CHS evaluate structural properties of the custody architecture. ERS reflects resilience against long-horizon degradation forces associated with Custodial Entropy. XRS reflects resilience against adversarial exposure surface conditions.

Conceptually, the Bitcoin Custody Resilience Index (BCRI) may be expressed as a function of the four analytical dimensions defined in this model:

$$BCRI = f(ARS, CHS, ERS, XRS) \quad (1)$$

where:
ARS = Architecture Resilience Score
CHS = Coordination Health Score
ERS = Entropy Resilience Score
XRS = Exposure Resilience Score

The specific functional form used to derive BCRI is defined within the BCRI assessment methodology and is not specified in this normative summary. As conceptually expressed in Equation (1), the Bitcoin Custody Resilience Index integrates architectural integrity, coordination durability, entropy resilience, and exposure resilience into a single bounded resilience outcome. This structure ensures that architecture strength, coordination durability, entropy resilience, and exposure resilience are evaluated as distinct but interacting dimensions of custody resilience.

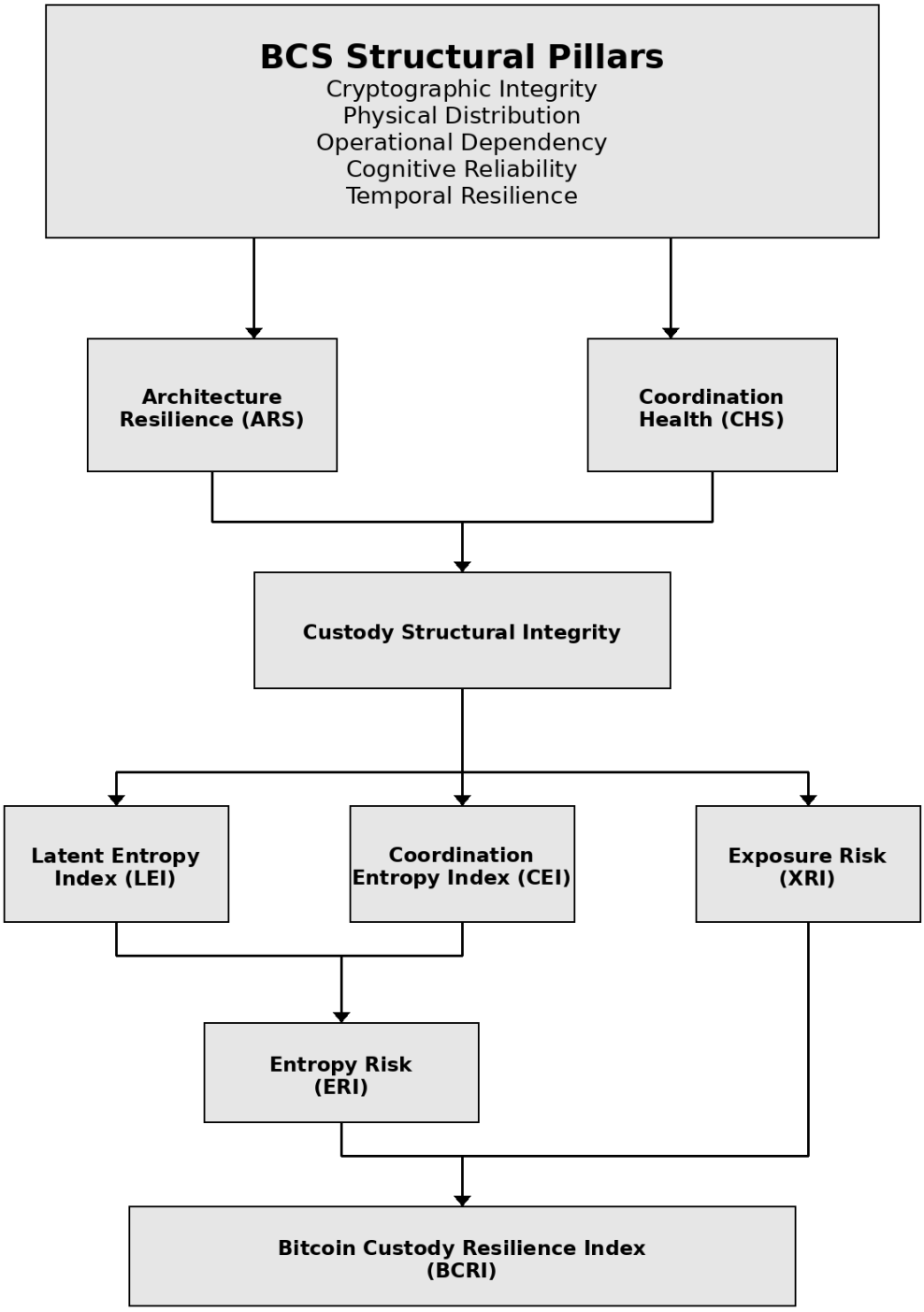

Figure 1 — BCS Structural Resilience Model. *BCS evaluates custody resilience as the interaction of architecture integrity (ARS), coordination health (CHS), entropy resilience (derived from ERI), and exposure resilience (derived from XRI).*

9. 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.

9.1 Assurance Tiers

BCS recognizes three Assurance Tiers, distinguished by the independence and rigor of the conformance evaluation process:

- **Self-Assessment**
  - *First-party, user-declared.*
  - Structured self-evaluation against published BCS criteria and BCRI scoring methodology. Valid only when performed honestly and without material omission. No independence or third-party review is implied.
- **Verified**
  - *Second-party evidence review.*
  - Documented evidence review by the BCS scheme owner or authorized reviewer. May include architectural documentation, recovery runbooks (non-sensitive excerpts), dependency disclosures, review cadence documentation, and signed attestation. Does not require disclosure of private keys. Does not constitute independent certification.
- **Independent Certification**
  - *Third-party conformity assessment.*
  - Formal third-party assessment conducted by an entity operationally and financially independent of both the operator and the BCS scheme owner. Not implied unless explicitly stated. No claim shall be made without formal third-party designation.

9.2 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.

9.3 Certification Threshold Logic

Catastrophic control failure conditions may vary depending on custody architecture classification and are defined within the applicable BCRI assessment modules.

Conformance evaluation under the Bitcoin Custody Standard requires that custody architectures satisfy defined structural and risk thresholds established within the BCRI assessment framework. These thresholds may include minimum structural resilience conditions and maximum acceptable risk exposure limits across relevant assessment dimensions.

Threshold values and interpretation bands are defined within the applicable BCRI scoring documentation and may vary depending on custody architecture classification and Assurance Tier. Failure to satisfy any required

structural or risk threshold shall result in non-conformance with the Bitcoin Custody Standard at the evaluated Assurance Tier.

9.4 Conformance Claim Statement

A custody architecture claiming conformance with the Bitcoin Custody Standard shall explicitly state:

- the applicable BCS version used for assessment;
- the declared Assurance Tier (Self-Assessment, Verified, or Independent Certification);
- the reported BCRI score and associated metric values (ARS, CHS, ERI, and XRI), where ERI and XRI represent the primary risk indicators from which ERS and XRS are respectively derived.

Conformance claims shall not imply applicability to future versions of the Bitcoin Custody Standard without reassessment. Where applicable, public conformance claims should reference the specific BCS document identifier and version number used for the assessment.

10. Proprietary Boundary Notice

Notice. The detailed scoring methodology, transformations, and threshold logic associated with the BCRI framework, including implementation of the Entropy Risk Index (ERI) and Exposure Risk Index (XRI), are proprietary and do not themselves constitute standalone normative requirements under BCS.

11. Stewardship and Research

The Bitcoin Custody Standard (BCS) is stewarded by the Bitcoin Custody Standard Initiative (BCSI). Stewardship includes maintenance of normative documents, publication of supporting research, and periodic revision of the standard to ensure continued alignment with evolving custody practices, technological developments, and emerging operational risks.

BCS research activities include ongoing analysis and publication of custody architecture resilience, entropy-related degradation mechanisms, and operational coordination challenges observed across real-world custody systems.

The BCS initiative welcomes constructive feedback and external contributions from researchers, practitioners, and industry participants. Contributions may include technical review, methodological suggestions, or empirical observations related to custody resilience.

Correspondence: contact@bitcoincustodystandard.org

Citation: Bitcoin Custody Standard Initiative. Bitcoin Custody Standard (BCS) — Normative Summary, Version 1.1 (BCS-NS-1.1), March 2026.