

# AI Decision Auditability Benchmark

*Aligned with VCP (VeritasChain Protocol)*

Version 1.0

A Common Standard for Measuring  
Algorithmic Trading Transparency

**Document ID:** VSO-SCORE-001

**Version:** 1.0

**Status:** Released

**Effective Date:** December 2025

**Publisher:** VeritasChain Standards Organization (VSO)

[veritaschain.org](http://veritaschain.org)

## 1. Overview

This benchmark provides a standardized framework for assessing the auditability of algorithmic trading systems. Rather than proposing technology adoption, it offers a common measure that organizations can use for self-assessment and third-party evaluation.

### 1.1 Purpose

**This is not an implementation proposal.** This benchmark enables organizations to diagnose their "auditability" (explainability) using an industry-standard measure. Results can be directly used as "evidence quality" for external audits and regulatory compliance.

### 1.2 Scoring System

Score	Meaning	Description
0	Not Implemented	Capability absent or fundamentally inadequate
1	Partial	Basic capability exists but with significant gaps
2	Full	Robust implementation meeting best practices

**Maximum Score: 20 points** (10 criteria × 2 points each)

## 2. Evaluation Criteria

The following 10 criteria are ordered by audit relevance, with evidence-centric criteria first and technical implementation details later.

### 1. Third-Party Verifiability

第三者検証可能性

**Core Question:** Can an external party independently recalculate and verify the audit trail?

Score	Criteria
0	No external verification possible; data is opaque or proprietary-only
1	Partial verification possible with vendor assistance or limited data access
2	Full independent verification using standard tools and published schemas

### 2. Tamper Evidence

改ざん検知

**Core Question:** Can unauthorized modifications to historical records be detected?

Score	Criteria
0	No tamper detection; records can be silently modified
1	Basic checksums or logs exist but gaps allow undetected changes
2	Cryptographic integrity (hash chains, Merkle trees) prevents undetected tampering

### 3. Sequence Fixation

順序の固定

**Core Question:** Is the chronological order of decision → order → execution immutably recorded?

Score	Criteria
0	Event ordering can be disputed or reconstructed post-hoc
1	Timestamps exist but lack cryptographic binding or independent verification
2	Monotonic sequencing (e.g., UUIDv7) with cryptographic linkage proves ordering

### 4. Decision Provenance

判断由来

**Core Question:** Can the inputs, conditions, and rationale behind each decision be traced?

Score	Criteria
0	Only outcomes recorded; no visibility into decision basis
1	Some inputs logged but incomplete or inconsistent coverage
2	Full provenance chain: market data, parameters, model state, and decision logic

## 5. Responsibility Boundaries

責任境界

**Core Question:** Is it clear who approved, modified, or overrode each action?

Score	Criteria
0	No attribution; actions cannot be traced to individuals or systems
1	Basic user logging but gaps in override tracking or delegation chains
2	Complete attribution with digital signatures for all approvals and overrides

## 6. Audit Submission Readiness

### 監査提出性

**Core Question:** Can a complete evidence package be exported for regulatory or audit review?

Score	Criteria
0	No structured export; manual data gathering required
1	Partial export capability; some data requires separate extraction
2	One-click export of standards-compliant evidence packages

## 7. Retention & Operational Durability

### 保持期間・耐久運用

**Core Question:** Are records retained for required periods (e.g., 7 years) with operational guarantees?

Score	Criteria
0	No formal retention policy; data may be lost or deleted
1	Policy exists but technical enforcement or monitoring is incomplete
2	Enforced retention with redundancy, integrity checks, and documented procedures

## 8. Timestamp Reliability

### 時刻の信頼性

**Core Question:** Are timestamps synchronized to a trusted, verifiable time source?

Score	Criteria
0	Local system clocks only; no synchronization or verification
1	NTP synchronization but no monitoring or drift detection
2	PTP or RFC 3161 timestamping with documented accuracy and monitoring

## 9. Cryptographic Strength

### 暗号強度

**Core Question:** Do signature and hash algorithms meet current security standards?

Score	Criteria
0	Weak or deprecated algorithms (e.g., MD5, SHA-1 for signatures)
1	Adequate algorithms but no key management or rotation procedures
2	Strong algorithms (Ed25519, SHA-256+) with documented key lifecycle management

## 10. Cryptographic Agility

暗号移行性 ( PQC準備 )

**Core Question:** Can the system migrate to new algorithms without breaking historical verification?

Score	Criteria
0	Hard-coded algorithms; migration would break verification
1	Algorithm identifiers exist but migration path untested
2	Documented migration procedure; backward compatibility verified for PQC transition

### 3. Self-Assessment Sheet

#	Criterion	Score (0-2)	Notes
1	Third-Party Verifiability		
2	Tamper Evidence		
3	Sequence Fixation		
4	Decision Provenance		
5	Responsibility Boundaries		
6	Audit Submission Readiness		
7	Retention & Operational Durability		
8	Timestamp Reliability		
9	Cryptographic Strength		
10	Cryptographic Agility		
<b>TOTAL</b>		<b>/20</b>	

#### 3.1 Score Interpretation

Score Range	Assessment	Recommendation
16-20	Strong Auditability	Ready for external audit and regulatory review
11-15	Moderate Auditability	Address gaps in 0-score areas before audit
6-10	Limited Auditability	Significant improvements needed; prioritize criteria 1-6
0-5	Inadequate	Fundamental gaps require immediate attention