ACQUISITION BRIEF

RealityAssurance.com

Version: 2026-01

Asset offered

- Domain: RealityAssurance.com

- Included (subject to agreement): domain name, associated website content and documents (if any), and related category materials created for the property.

- Intended use: neutral, vendor-independent category reference.

Not included

- No insurance activity, no underwriting, no brokerage, no "coverage" or "policy" offering.

- No certification service, no audit service, no legal/compliance advice.

- No company, no liabilities, no staff, no customer contracts.

Contacts

- Stewardship, research collaboration, or acquisition inquiries: contact@realityassurance.com

This document

- Audience: institutional buyers, standards initiatives, audit and assurance leaders, regulated-industry stakeholders, and public-interest governance teams.

- Purpose: describe the category, the holding pattern, and why the asset can become a category-grade banner.

Informational notice

Disclaimers (must remain identical everywhere)

1. Decision in one page

Category statement

Reality Assurance is emerging as the institutional layer that connects provenance signals and transparency obligations with audit-ready governance evidence.

Canonical definition (use this exact sentence)

Reality Assurance is the set of controls, evidence, and independent assessment practices that provide justified confidence that a digital interaction or record reflects an authorized real-world event, within a defined scope and threat model.

Problem it captures

In a synthetic-by-default environment, images, audio, video, documents and signals can be generated or altered at scale. Default trust collapses. Organizations need repeatable evidence that can survive audits, disputes, and third-party scrutiny.

Why now (converging drivers)

- Transparency obligations and implementation work are pushing marking and disclosure expectations for synthetic content.

- Provenance standards (e.g., Content Credentials) are being deployed operationally, making signed provenance "real-world usable".

- Governments are explicitly shaping trusted third-party AI assurance markets, making "assurance" procurement language.

- The "wild-west" phase of AI audit/assurance is being pressured toward standardization and credible practice boundaries.

Why the domain can command strategic value

Category-grade domains gain value when multiple stakeholders need a neutral banner that can be referenced without vendor lock-in. Reality Assurance sits above provenance building blocks and below legal, reputational, and financial risk decisions. It is board-readable, procurement-readable, and cross-sector.

Strategic buyer set (solvable)

- Audit and assurance leaders (Big 4 and independent assurance firms)

- Hyperscalers, security platforms, and identity/provenance infrastructure providers

- Insurers and reinsurers (risk frameworks and underwriting prerequisites, without the site selling insurance)

- Governments, regulators, and public-interest initiatives (guidance portals, registries, procurement language)

Safe holding pattern (legal posture)

- Use "assurance" in the NIST sense: measurable justified confidence that controls work as intended (not "insurance").

- Never present the site as an insurance provider, broker, or underwriting entity.

- Remain vendor-neutral and descriptive; avoid any implication of official certification or affiliation.

2. What the category covers (scope)

Reality Assurance is broader than "content authenticity" alone. Within defined boundaries, it covers:

- Media and documents used as evidence (claims, investigations, compliance records)

- Identity and presence signals (who acted, who approved, who authored)

- Sensor and measurement feeds (industrial, climate, security contexts)

- Agentic workflows (inputs, outputs, logs, decision traces)

Four pillars (board-friendly)

1) Marking and disclosure (human- and machine-readable signals)

2) Provenance and cryptographic binding (claims, signatures, manifests)

3) Verification and independent assessment (repeatable checks, trusted assessment models)

4) Assurance cases and governance evidence (structured argument plus evidence for acceptable risk)

What it is not

- Not a product, not a certification scheme, not a regulator portal (unless acquired and operated as such).

- Not an insurance offering and not a substitute for legal/compliance/audit professionals.

- Not a promise of truth; it is a framework for justified confidence under a defined threat model.

3. Use cases (illustrative)

- Audit-ready evidence for synthetic or manipulated media used in claims, disputes, investigations, and regulated reporting.

- Enterprise procurement: "assurance-ready" evidence artifacts attached to AI systems and workflows.

- Agentic systems: action trails and decision traces that remain reviewable after incidents.

- Measurement integrity: sensor feeds and operational signals that influence safety, compliance, or public outcomes.

4. Deployment options for an acquirer

Option A: Public reference hub (category stewardship)

- Definitions, taxonomy, reference links, and "what good evidence looks like".

- Designed to be citeable without vendor endorsement.

Option B: Assurance practice or ecosystem program (non-exclusive language)

- Host guidance, assessment patterns, and assurance-case templates.

- Position as "audit-ready reality evidence" without claiming certification authority.

Option C: Government or public-interest portal

- Procurement language, public guidance, registries, and transparency references.

Option D: Industry foundation / consortium umbrella

- Neutral vocabulary alignment across platforms, media, and verification tooling.

5. Acquisition process (clean, institutional)

- Step 1: Initial contact with buyer profile and intended stewardship model.

- Step 2: Optional NDA, then high-level alignment on scope, non-goals, and legal posture.

- Step 3: Commercial terms, transfer method, and post-transfer content governance (if any).

- Step 4: Domain transfer and handover of documents/assets per agreement.

Initial contact: contact@realityassurance.com

Primary references (selected)

- NIST CSRC Glossary: Security Assurance

  https://csrc.nist.gov/glossary/term/security_assurance

- EU AI Act (practice resource): Article 50 transparency obligations

  https://aiactservice-desk.europa.eu/ai-act-implementation/1-getting-started/ai-act-legal-text/article/article-50-transparency-obligations-providers-and-deployers-certain-ai-systems_fr

- European Commission: work on code of practice for marking and labelling AI-generated content

  (reference PDF summary)

  https://dpo-india.com/Resources/European_Commission/Commission-launches-work-code-practice-marking-labelling-AIgenerated-content.pdf

- UK DSIT (GOV.UK): Trusted third-party AI assurance roadmap

  https://www.gov.uk/government/publications/trusted-third-party-ai-assurance-roadmap/trusted-third-party-ai-assurance-roadmap

- C2PA: Content Credentials Technical Specification

  https://c2pa.org/specifications/specifications/2.3/specs/C2PA_Specification.html

- BSI: UK AI audit standard market signal (press release / coverage references)

https://www.bsigroup.com/en-GB/insights-and-media/media-centre/press-releases/